HACK X CRACK: ROOTKIT = LA PESADILLA DE CUALQUIER ADMINISTRADOR



APRENDE A COMPILAR

HA LLEGADO EL MOMENTO DE ENFRENTARTE A UN COMPILADOR, PASO OBLIGADO ANTES DE EXPLICARTE LOS EXPLOITS

QUÉ OPINAN LOS HACKERS



DE LA PIRATERÍA EN INTERNET

¿DE DÓNDE SALEN LOS BUGS?

COMPRAS POR INTERNET: ¿TENEMOS LA SOLUCIÓN?

DE PROFESIÓN: CRACKER ELLOS NOS OBLIGARON

ELLOS TE ENSEÑAN LA SUPERFICIE



NOSOTROS "EL RESTO"

Nº 5 -- P.V.P. 4,5 EUROS

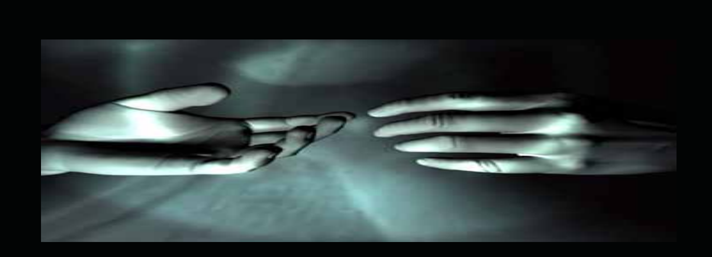


HACK X CRACK - HACK X CRACK - HACK X CRACK - HACK X CRACK

LOS CUADERNOS DE HACK X CRACK

www.hackxcrack.com

ROOTKITS SIN DEFENSA POSIBLE



HEMOS PUESTO UN SERVIDOR A TU DISPOSICIÓN

HACKEANOS !!!

PENETRACIÓN DE SISTEMAS POR NETBIOS

COMPILACIÓN DEL NETCAT CON OPCIONES "ESPECIALES"

NETBIOS: UN AGUJERO DE SEGURIDAD NO RECONOCIDO POR MICROSOFT

EDONKEY 2000 SOFTWARE GRATIS!!!

HACK: NETBIOS, UN REGALO DE BILL GATES PARA LOS HACKERS



LOS CUADERNOS DE HACK X CRACK
www.hackxcrack.com

EDITORIAL: EDITOTRANS S.L.
C.I.F: B43675701

Director Editorial
I. SENTIS

E-mail contacto
director@editotrans.com

Título de la publicación
Los Cuadernos de HACK X CRACK.

Nombre Comercial de la publicacíón
PC PASO A PASO

Web
www.hackxcrack.com

Deposito legal: B.26805-2002
Código EAN: 8414090202756
Código ISSN: En proceso



Director de la Publicación
J. Sentís

E-mail
director@hackxcrack.com

Diseño gráfico:
J. M. Velasco

Contacto diseñador gráfico
grafico@hackxcrack.com

Redactores
AZIMUT, ROTEADO, FASTIC, MORDEA, FAUSTO, ENTROPIC, MEIDOR, HASHIMUIRA, BACKBONE, ZORTEMIUS, AK22, DORKAN, KMORK, MAILA, TITINA, SIMPSIM... ... ...

Contacto redactores
redactores@hackxcrack.com

Colaboradores
Mas de 130 personas: de España, de Brasil, de Argentina, de Francia, de Alemania de Japón y algún Estadounidense.

Contacto colaboradores
colaboradores@hackxcrack.com

Imprime
I.G. PRINTONE S.A. Tel 91 808 50 15

Distribución
Coedis S.L. Avda. de Barcelona 225. Molins de Rei. Barcelona. Tel 93 680 03 60 FAX 93 668 82 59
WEB: www.coedis.com (mapa de distribución en la web)

NUMERO 5 -- PRINTED IN SPAIN
PERIOCIDAD MENSUAL

DECLARACION DE INTENCIONES

PARA "LOS OTROS":

1.- La intención de la presente publicación NO ES fomentar la piratería informática ni la "delincuencia" en la Red.
2.- Cualquier texto publicado es VALIDADO por nuestra Asesoría Jurídica, por lo que advertimos a cualquier persona, empresa u organización de la inutilidad de cualquier iniciativa jurídica en nuestra contra. Aun así, en caso de cualquier iniciativa en contra de esta revista, deberá ser debidamente presentada y resuelta en la Razón Social que figura en nuestros documentos de constitución.
3.- Esta publicación no se hace responsable del mal uso de los conocimientos que se exponen.
4.- Esta publicación NO FACILITARÁ los datos de nuestros colaboradores ni el origen de nuestros conocimientos salvo ORDEN JUDICIAL y, aun así, advertimos que algunos de esos colaboradores NO SON CONOCIDOS mas que por sus NICKS (alias). Por ello, correrá a cargo de los organismos pertinentes su "descubrimiento".
5.- Esta publicación NO SE HACE RESPONSABLE ni tienen por qué COMPARTIR las opiniones personales vertidas por sus colaboradores, por lo que NO SOMOS RESPONSABLES de las mismas.
6.- Cualquier texto publicado estará bajo las protecciones de DERECHOS DE AUTOR y no se permite su copia, publicación, modificación o distribución sin antes obtener el permiso de esta editorial. De este punto quedan exentos aquellos textos que han sido obtenidos de terceros y/o que están sujetos a otras licencias (ya sean por parte de su autor o por terceros).
7.- Si desean ponerse en contacto con nuestro departamento jurídico, rogamos enviar mail a juridico@hackxcrack.com

PARA NUESTROS LECTORES:

Como podréis ver, esta no es una revista mas, por primera vez tenéis ante vosotros una publicación LIBRE que os ofrecerá la posibilidad de explorar la red tal y como debe explorarse ;)

Esta publicación responde a la pregunta mas veces expuesta en LA RED: ¿Como puedo ser un hacker? Bien, ahora seguro que muchos ya se están "sonriendo" y pensando lo ilusos que somos al intentar "eregirnos" en "portadores de LA LUZ", pensando que seremos una "escuela de lamers" y similares a otras publicaciones que, entre sus 100 páginas de revista solo contiene 5 de "material utilizable" (si es que puede llamarse así).

Pues NO, lo siento, vosotros seréis nuestros jueces y, llegado el caso, NUESTROS VERDUGOS.

Nuestro objetivo es: ACABAR CON LA BASURA DE LA RED (lamers y demás "esencias") con el único método que conocemos: LA EDUCACIÓN y con un única bandera que será por siempre nuestra firma: SOLO EL CONOCIMIENTO TE HACE LIBRE.

Estos son nuestros pilares: LA EDUCACIÓN Y EL CONOCIMIENTO. Para ser un HACKER (maldita palabra mal entendida por unos y peor utilizada por otros) solo hace falta dos cosas: curiosidad y medios, a partir de ahora la curiosidad deberéis ponerla VOSOTROS, porque los medios los facilitaremos NOSOTROS. En las siguientes líneas os descubrimos cómo podremos conseguir nuestros objetivos y definimos algunas de las palabras que más han sido violadas y retorcidas en su significado.

Hacker: Este término ha sufrido a lo largo de su corta historia una horrible conspiración perpetrada por la ignorancia de los medios, eso que personalmente llamo "periodismo de telediario" (en clara alusión a los ridículos artículos que no hacen mas que intoxicar nuestra percepción de las cosas e insultar nuestra inteligencia). Ese tipo de periodismo unido a "otros poderes", desde los monopolios que deben justificar su incompetencia hasta los gobiernos que deben justificar sus intereses ocultos pasando por la industria del cine (normalmente demonológica) y los medios informativos "de masas".

Pues bien, HACKER no es mas que una persona que posee conocimientos avanzados sobre una materia en concreto, normalmente relacionados con la tecnología aunque ni mucho menos limitado a ello. Ponen sus aptitudes al servicio de un único objetivo: EL CONOCIMIENTO. Desean conocer el funcionamiento de "las cosas" y no encuentran límites en sus camino mas que su propia curiosidad. No se dedican a destruir ni a causar estragos entre sus "victimas", no se dedican a robar ni a chantajear ni a regodearse de sus "conquistas", muy al contrario suelen advertir a terceros de las debilidades de sus sistemas y, desgraciadamente, esos "terceros" en lugar de agradecerles su aviso se dedican a denunciarlos o perseguirlos… aunque no siempre es así, por supuesto, muchas compañías y gobiernos han aprendido lo valiosos que son los HACKERS y ahora algunos son colaboradores (o empleados) de estos. **BILL GATES** es un HACKER (el papá ventanas), como **Linus Torvalds** (el papá Linux) o **Grace Hooper** (la Almirante, creadora del Lenguaje COBOL), los autores del COREWAR **Robert Thomas Morris, Douglas McIlroy** y **Victor Vysottsky** (precursores de los creadores de virus informáticos), **Fred Cohen** (el primer investigador y autor de los virus de la historia), **Dennis Ritchie** y **Ken Thompson** ("hacedores" del Lenguaje C y co-creadores del SO UNIX), **Gary Kildall** (autor del sistema operativo CMP y CPM/86), **Tim Paterson** (autor del Quick & Dirty DOS), **Morris** (autor de "The tour of the Worm"), **Kevin Mitnick** (el más buscado por el FBI), **Phiber Optik** (líder juvenil convertido en símbolo de los hackers), **Richard Stallman** (impulsor del "software gratuito" y GNU), **Johan Helsingius** (primer conductor de un Remailer Anónimo), **Chen Ing-Hou** (autor del virus CIH -Chernobyl-), **Sir Dyistic** (creadorutor del Back Orifice), **David L. Smith** (virus Melissa), **Reonel Ramonez** (virus LoveLetter), **Vladimir Levin** (Robó electrónicamente 10 millones de dólares al Citibank), y muchos mas. ¿Cómo? ¿Pero no hemos dicho que los hackers no comenten delitos? Pues NO, vuelve a leer su definición… pero claro, de todo hay en la viña del señor, y al igual que hay delincuentes entre el clero hay hackers que en un momento u otro han ·caido· en la ilegalidad, nadie es perfecto!!!!! … y **Bill Gates** es un HACKER? Por supuesto, solo tienes que leerte su biografía. ¿Sorprendido? Espero que no, porque eso no es nada mas que un cero a la izquierda en comparación con lo que vas a encontrar en esta revista.

EDITORIAL:
... EL CAMINO SE HACE AL ANDAR ...

Bueno, bueno, bueno... un mes más en el quiosco y con este ya son CINCO! Esta vez seremos breves, que nuestras editoriales parecen clases de historia :)

Ante todo agradeceros todo el apoyo que día a día recibimos y saludar a las personas que han contestado a nuestra "oferta de empleo". La verdad es que necesitamos vuestra ayuda, porque la gestión necesaria para seguir adelante cada vez es mayor y eso está afectando a la calidad de los textos. Supongo que las editoriales "normales", proteccionistas hasta la saciedad nunca dirían cosas como estas, pero ya nos conoces, nosotros solemos informar tanto de lo bueno como de lo malo, no hacemos como Aznar que se esconde detrás de sus ministros y no es capaz de reconocer nada de nada... je, je... quien diría que el que escribe esta editorial tenía hasta hace poco el carnet del P.P. ¿verdad? Pues sí, lo tenía, pero ya nunca más me engañarán... a partir de ahora quien quiera mi voto que me regale una pantalla TFT de 22" :)

Mas cosas, esta vez para los quiosqueros. Hemos recibido mails en los que nos comentan que la editorial del número 4 fue un poco "dura" en relación a los problemas de distribución. Pues la verdad, tienen razón, hay verdaderos profesionales en el sector, nos lo han demostrado (aunque en toda casa hay "ovejas negras" y por desgracia se suelen hacer notar más). Debo decir que poco a poco aprendemos de nuestros errores y nos damos cuenta que nunca una mala distribución es por causa de un solo sector... pero no sigo hablando que me cargo a los distribuidores y entonces si que la revista no ve la luz nunca más.

Bueno, espero que os guste este número y para el siguiente vamos a mejorar bastante, ya verás... mejoraremos en la Web, en la revista, en los envíos, en los textos...

Un abrazo muy fuerte a todos y gracias por leernos ;)

INDICE

HACK-OPINION
LA PIRATERIA EN INTERNET

Existe una solución para acabar con la piratería del Software de Aplicaciones, pero los que tienen la sartén por el mango parece que hacen oídos sordos. Señores, si no nos quieren escuchar, después no vengan llorando.

Sobre mi persona...

El que escribe estas líneas no se considera un hacker, lo siento, hacker es algo que otros te llaman, no algo que tú te puedas considerar.



"…ser Hacker significa mantener vivo el deseo de "conocer"…"

Las opiniones que expondré en este texto no representan a la posible existencia de una comunidad hacker en tanto que tal comunidad no existe. Los que son llamados hackers son simples mentes curiosas y eternos aprendices de cuanto les rodea, son como cualquier otra persona y en tanto que no existe una comunidad de mentes curiosas hablo en mi propio nombre.

El ser humano es, en sí mismo y desde su nacimiento, un espécimen sediento de saber, es una lástima que durante su crecimiento pierda lentamente esa sed y acabe formando parte de una sociedad parametrizada e insulsa.

Para mi, ser Hacker significa mantener vivo el deseo de "conocer", ser siempre ese niño pesado que no deja de preguntar por el mundo que le rodea... quizás a eso se refieren algunos escritos cuando te advierten que debes ser como un niño para obtener la verdadera felicidad.

Qué es La Piratería.

Dejando a un lado "lo que soy", que eso es lo de menos, vamos a reflexionar sobre esa gran mentira llamada Piratería Informática. Todo lo que alegaré en este texto se refiere al Software de Aplicaciones, esos que diariamente utilizamos, no a la música ni a los juegos ni a los videos, tenlo muy en cuenta, no perderé mi tiempo dando ideas a las multinacionales del entretenimiento sobre cómo deben dirigir sus negocios, simplemente me da igual lo que hagan o dejen de hacer... bueno, mentira, que sigan sacando nuevas fórmulas "anti-copia" para que yo pueda seguir disfrutando de sus retos ;)



"…En mi opinión, piratear significa sacar beneficio económico del trabajo de otras personas…"

 HACK-OPINION: LA PIRATERIA EN INTERNET

En mi opinión, piratear significa sacar beneficio económico del trabajo de otras personas. No quiero entrar ahora en asuntos sociales, puesto que esa definición incluiría al propio estado como El Gran Pirata, así que vamos a concretar. Piratear es simplemente coger algo que no es tuyo y sacar beneficio económico de ello, es decir ROBAR. Aplicado al software, piratería es pillar un programa como photoshop, hacer 600 copias y vendérselo a un tercero, así de claro y sencillo, sacar un beneficio de algo que no te pertenece. Esto es un delito perfectamente contemplado en la ley y cualquiera que se dedique a ello debería ser castigado. Ten en cuenta que he hablado de beneficio económico.

Qué no es La Piratería.

No es piratería utilizar un recurso ajeno para fines no lucrativos siempre y cuando no limites en forma alguna el uso y disfrute del mencionado recurso por parte de su propietario.

Si duplicas/copias un programa y lo utilizas para tu uso personal, desde mi punto de vista no estás cometiendo perjuicio alguno en tanto que no estás obteniendo beneficio económico ni estás dañando el objeto original y por supuesto no estás limitando el uso del mismo a su propietario..

Ahora seguro que he levantado dolorosas ampollas en muchos lectores que trabajan de programadores o similares... por favor, no quemes la revista, dame la oportunidad de explicarme y quizás acabemos siendo amigos.

Solución a la "piratería".

No es que yo sea dios, faltaría más, pero hace más de 10 años que trabajo de programador y más de 6 que estoy en una de la multinacionales más importantes. Este "status" me ha permitido recorrer la cadena que sigue un producto (programa) desde sus inicios hasta su puesta en la calle y puedo asegurarte que existe una solución para acabar con la piratería, multiplicar las ventas de cualquier software y hacer ganar a las empresas de software más dinero que hasta ahora.

Actualmente, muy pocos son los usuarios que compran productos profesionales, prefieren "pillarlos" de Internet y copiarlos. El motivo está claro: El Precio. Hay que estar loco (o ser envidiablemente rico) para comprar productos que cuestan los dos ojos de la cara, un riñón y parte del hígado. Si encima quieres ese programa simplemente para aprender a utilizarlo, no para obtener beneficios económicos, pues ni te planteas la posibilidad de comprarlo.



"... una versión para "todo el mundo" a 6 euros..."

Solución: Sacar al mercado dos versiones de los programas. Una versión para "todo el mundo" a 6 euros (por ejemplo) y la misma versión a 600 euros. La primera sería una simple

 HACK-OPINION: LA PIRATERIA EN INTERNET

cajita sin instrucciones impresas ni soporte por parte del fabricante, es decir, una versión económica. La segunda sería para quienes desean soporte, manuales impresos, etc, es decir, para las empresas que utilizarán ese software de forma intensiva y obtendrán beneficios por su empleo.

Antes de que me quemes en la hoguera, piensa un poco, que yo he sido autónomo y se lo que es tener una mini-empresa y se que lo que acabo de decir habrá "calentado" tanto a los programadores (recalentado) como a los pequeños empresarios. Parece que me guste crearme enemigos, pero te aseguro que todo esto tiene un objetivo, dame un margen de confianza, por favor.

Reflexionando sobre la propuesta: Usuarios "caseros".

Empecemos por los usuarios caseros. A todo el mundo le gusta tener un programa original y olvidarse por 6 euros de los peligros del "pirateo". Olvídate de los virus, troyanos, sospechosas modificaciones de código, tediosas descargas, búsqueda y aplicación de cracks, gastar dos o tres CD´s para copiarlo (todos sabemos que no es sencillo acertar a la primera), problemas con las actualizaciones en las Webs oficiales y en definitiva inútiles pérdidas de tiempo por todos lados. Yo aprecio cada segundo de mi vida y te aseguro que pago gustoso 6 euros por no tener que perder mi tan preciado tiempo.

Pero es que eso no es todo, si esta propuesta fuese una realidad, la Informática e Internet serían un medio que disminuiría la brutal diferencia de "posibilidades" que hoy en día existe entre las personas. Tanto si se te caen los billetes de 500 euros al andar como si estás mas bien escaso de medios, podrías aprender a utilizar esos programas que quizás en un futuro te servirán para encontrar trabajo y labrarte un espléndido futuro.

Desde el punto de vista de la empresa creadora del software, se podrían preparar para las ventas masivas de sus productos. Aumento de ventas, promoción automática del programa y CERO en gastos de asistencia al cliente puesto que estamos hablando de la versión económica.

Reflexionando sobre la propuesta: Empresas.

Aquí tenemos a dos grupos perfectamente diferenciados:
- los que explotarán el software al 90%, necesitan de un buen soporte al cliente, quieren manuales impresos e incluso amplían su licencia para acceder a cursos de aprendizaje, extensiones especiales de asistencia, y todo lo que puedas imaginar.
- los que tienen un pequeño negocio, no pueden pagar esos precios desorbitados y no necesitan asistencia porque no utilizarán ni un 25% de las capacidades del programa.

Los primeros deberían adquirir el producto y pagar por todos esos extras que necesitan. Los segundos, normalmente pequeños empresarios, podrían adquirir el producto económico.

Seamos realistas, no puedes pedirle a una empresa de software que te de soporte por seis euros, eso no es posible. Así que si no tienes dinero para pagar 600 euros, al menos puedes comprar la versión económica y obtener "soporte" en los foros que normalmente se crean los usuarios para ayudarse unos a otros y compartir experiencias.

Para las empresas creadoras de software, esto significaría "descargar" de trabajo a sus departamentos de soporte y economizar recursos, lo que provocaría un aumento en la calidad del soporte ofrecido a los compradores

HACK-OPINION: LA PIRATERIA EN INTERNET

del producto en su versión "con soporte".

Seamos sinceros, todo el mundo conoce y/o trabaja hoy en día con Microsoft Office, según el último estudio existen más paquetes Office instalados que ventas de Windows... es decir, que hay gente que tiene el office instalado en la nevera de su casa, porque si no tienes un Windows ya me dirás dónde tienen instalado el Office. Resumiendo, que SOMOS UNOS PIRATAS DE CUIDADO, que la población española ha decidido de un día para otro transformarse en delincuentes, somos tan tontos que hemos decidido ser carne de prisión y delinquir "por gusto"... venga hombre, cuando algo así sucede, cuando la mayoría emplean medios "paralegales" para obtener "algo" es porque SE LES HA EMPUJADO A HACERLO.



"... no obliguemos a la gente a "delinquir", dale a la gente la oportunidad de hacerte rico, dadnos a los pobres mortales la posibilidad de pagar..."

* Señores, seamos serios.
Vamos a ver, seamos inteligentes y no obliguemos a la gente a "delinquir", dale a la gente la oportunidad de hacerte rico, dadnos a los pobres mortales la posibilidad de pagar, que parece que nadie se entera. A nosotros, a ti y a mi, no nos gusta correr el riesgo de que un buen día un juez dicte una orden y un grupo de policías entre en nuestra casa y nos detenga por "posesión" de "software pirata", que a nadie le gusta correr riesgos pero, claro, si me quieres cobrar por un programa un precio que representa el "curro" de tres meses, pues no señor, lo siento, tendré que correr "riesgos".

Señores directivos, piensen un poco. Urg!!!! Ahora estoy hablando conmigo mismo, yo soy directivo, lastima que no puedo tomar ese tipo de decisiones... :(A todo el mundo le gusta "poseer", pues hombre, ofrece un precio que pueda pagar.
Vamos a poner un ejemplo de un caso real que me encontré hace mucho y cuya "escena" se ha venido repitiendo constantemente:

- Por un lado tenemos a una gran empresa de enseñanza nos pide 300 licencias para un programa al precio estipulado, le hacemos un sustancioso descuento y ofrece sus cursos a nivel estatal con sucursales en las principales ciudades españolas a un precio de, por ejemplo, 600 euros por curso.
- Por otro lado tenemos a una pequeña empresa de enseñanza de una diminuta localidad que nos pide 10 licencias para su único y pequeño local de enseñanza, le hacemos un ridículo descuento y ofrece sus cursos a 200 euros.

Señores aquí falla algo, la primera empresa obtiene un precio económico para ofrecer cursos a un alto precio en zonas privilegiadas y la otra, obtiene el mismo software a un precio 3 veces superior para ofrecer cursos a un precio realmente económico en zonas poco céntricas. En mi opinión, la segunda empresa casi está

 HACK-OPINION: LA PIRATERIA EN INTERNET

haciendo una labor social por la cual el estado debería pagarle y en cambio no solo nadie le ayuda sino que encima le ofrecen el software mucho más caro. Pues no se extrañe nadie de la situación que vive España, uno de los países con mayor índice de copias ilegales del planeta.

¿Existen soluciones? Pues claro que sí, siempre existen soluciones, desde subvenciones (esa solución no me gusta) hasta políticas de comercio basadas en "la realidad", es decir, que una pequeña empresa pueda obtener, como mínimo, los mismos precios que obtienen las grandes, y no me digas que eso es difícil de gestionar, no señor, eso lo hago yo cada día y te aseguro que en base a los resultados económicos de las empresas y su ubicación geográfica puedes perfectamente aplicar tarifas distintas e incluso justas.

Señores, ¿quieren acabar con la piratería?, pues apliquen las políticas de comercialización adecuadas y dejen de llorar.

Experiencia real:

Un día me vino un conocido (un buen amigo) y me dijo que había comprado un programa y que no le funcionaba, que el lector de CD no podía leerlo. Al introducir el CD en mi PC el resultado fue el mismo, se iniciaba la instalación del programa pero decía que introdujésemos el disco original. Después de un par de escarceos por el google pudimos ver que no éramos los únicos, que la compañía había incorporado a los CDs un sistema de seguridad que en el 20% de los casos aproximadamente impedía que el comprador legítimo del software pudiese instalarlo.

Mi amigo me trajo el CD porque conocía mis "especiales gustos" a la hora de disfrutar de la vida, no hay nada mejor que un buen sistema de protección que, digamos, estudiar ;). Después de dos días y mucha diversión mi amigo pudo instalar su programa ;) Por cierto, dos meses después la compañía creadora del software ponía en su Web un CRACK para que los usuarios legítimos pudiesen instalar sus programas, bueno, ellos lo llamaron "parche" pero después de pasar por mis manos y estudiarlo un poco puedo decir con un 100% de seguridad que era un CRACK.

Esta situación provocó dos cosas. Por un lado, mi amigo, aficionado a la informática desde la cuna (por eso nos hicimos amigos), estuvo conmigo todo el fin de semana viendo cómo conseguí instalar el programa; ahora es un cracker consumado y yo a su lado soy una lombriz. Por otro lado, nunca más ha comprado un programa original... bueno, mentira, compra cualquier programa que anuncia tener un nuevo sistema anticopia para... (sin comentarios). Es decir, las empresas de software se gastan millonadas en investigar sistemas que protejan sus programas y el resultado es que transforman a personas normales en verdaderos crackers. Señores, algo falla ¿verdad?.



Recuerda una ...

Recuerda una cosa que hemos indicado al principio, por favor: todo este texto hace referencia al Software de Aplicaciones, no hace referencia al "software" lúdico (juegos, música o video…)

Despedida:

El que escribe estas líneas tiene su opinión personal sobre el problema del pirateo de software lúdico, pero no osaría exponer argumento alguno en tanto que mi experiencia se basa en el Software de Aplicaciones. Considero que uno no debe hablar de aquello que desconoce, incluso aunque trabajes diariamente en temas aparentemente similares, uno debe basar sus propuestas en lo que

 HACK-OPINION: LA PIRATERIA EN INTERNET

realmente "toca" cada día, nada más.

Quizás pienses que soy demasiado estricto, pero no soporto las tertulias ni los telenoticias (el tonto-diario). Fíjate bien en lo que es una tertulia hoy en día: un moderador reúne en una mesa a 5 "periodistas" y va sacando temas e instando a que esos cinco señores opinen sobre el tema expuesto, es algo tan absurdo como coger a un chimpancé y pedirle que te recite una poesía. Cada uno tiene una experiencia en la vida, esa experiencia te permite hablar sobre aquello que conoces de primera mano, aquello que has experimentado en tus propias carnes, sobre los trabajos que has tenido, etc; pero no puedes ser un especialista en todo, es absurdo que una persona hoy hable de la guerra y mañana de no se qué situación política en no se qué país y pasado mañana de la educación y el otro de economía, genética, historia, patrones sociales, medidas anticorrupción… … … … … … lo que me molesta no es que se hable de ello, sino la seguridad con que lo hacen, convencidos de cada uno de sus argumentos, como si fuesen verdaderos especialistas en cada una de las materias sobre las que debaten. Es increíble, de verdad. Y ya no me meto con los telediarios porque se me acaba el espacio…

… … bueno, solo una cosa: El colmo de un informático no es, ni de lejos, que en su trabajo se vea obligado a convivir con Windows, je, je, ni de lejos, el colmo de un informático es tener que soportar la retransmisión de una noticia relacionada con los ordenadores, es monstruoso, horrible, peor que cualquiera de las creaciones de lovecraft.

Llegó en momento de despedirme esperando que a partir de ahora no creas todo lo que cuentan los medios informativos sobre la piratería. No espero que comulgues con mi forma de ver las cosas, solo pretendo demostrar que existen alternativas de aplicación real para acabar con los problemas más complejos… solo hace falta un poco de imaginación y ganas de cambiar las cosas.



"…es absurdo que una persona hoy hable de la guerra y mañana de no se qué situación política en no se qué país y pasado mañana de la educación y el otro de economía, genética, historia, patrones sociales, medidas anticorrupción…"

ROOTKITS: LA PESADILLA DE CUALQUIER ADMINISTRADOR

OCULTACIÓN DE PROCESOS. OCULTACIÓN DE DIRECTORIOS.
OCULTACIÓN DE ARCHIVOS. OCULTACIÓN DE CONEXIONES.

PARTE I: ¿QUÉ ES UN ROOTKIT?

1.- La definición:

La definición de rootkit que podemos encontrar por Internet o que nos dará cualquier persona se parecerá bastante a lo siguiente: "Conjunto de herramientas que los Hackers utilizan para conseguir derechos de ROOT, crear puertas traseras y ocultar sus actividades.

Vale, eso está muy bien, pero vamos a acercarnos un poco más a la realidad. Un rootkit no es un escaneador de redes, ni un xploit, ni una herramienta de gestión de redes, ni un virus, ni un troyano, ni nada de lo que puedes encontrarte un buen día en tu PC... un rootkit es mucho más que todo eso. Limitarnos a definir "una cosa" diciendo lo que no es sería muy conservador por nuestra parte, así que, como siempre, daremos nuestra opinión "personal": Un rootkit es un código (programa) que al ser ejecutado en el ordenador-victima provocará una redirección y/o sustitución de binarios, hablando claro, provocará cambios en los ejecutables del sistema (o simplemente los sustituirá).



La utilización de...

La utilización de rootkits es una agresión directa contra la integridad del sistema intervenido, acabamos de decir que modifica o parchea los archivos del sistema; por lo tanto no te recomendamos utilizar este tipo de técnicas salvo que sepas perfectamente lo que estás haciendo.

2.- Comprendiendo las posibilidades:

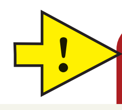
- Si, pero no acabo de entenderlo, explícame más.

Vale. Vamos a poner un ejemplo que ya conocemos. Cuando hacemos un listado de directorios desde una Ventana de Comandos con el comando dir (ampliamente utilizado y explicado en anteriores números), obtenemos el listado de los directorios y archivos de la ruta especificada. Cuando hacemos un dir/a obtenemos un listado de los directorios y carpetas pero esta vez también podremos ver los directorios y carpetas que tienen el atributo de oculto.

Imagina que alguien sustituye el código del comando dir (el binario que "contiene" el comando dir o cualquier otro archivo que afecte a dicho comando) por otro aparentemente idéntico. Imagina que, aparentemente, el comando dir se comporta de forma idéntica a como lo ha hecho siempre pero tiene una nueva "utilidad" activada por defecto, por ejemplo, ocultar cualquier directorio que empiece por _oculto_. ¿Te das cuenta del poder que te ofrece esa posibilidad? Pues eso (y otras muchas cosas) es lo que puede hacer un rootkit cuando se ejecuta en una "víctima", modificar el sistema operativo para obtener nuevas "opciones" ;)

Imagina que encontramos un servidor con el

ya explicadísimo code/decode bug, imagina que subimos un rootkit cuya función es ocultar cualquier proceso que empiece por _oculto_, imagina que una vez subido ejecutamos el rootkit. Se acabó!!!! Desde ese momento podrás crear una carpeta en el directorio raíz C:\ que empiece por _oculto_ (por ejemplo _oculto_esteesmidirectorio) y el administrador del equipo será incapaz de verla. No importa el método que emplee para listar los archivos ni las opciones del sistema operativo que active, esa carpeta y su contenido, simplemente, no existe: solo tú conoces su existencia.



Una manera de...

Una manera de "descubrir" esos archivos es iniciar el PC afectado con un Sistema Operativo distinto (Linux por ejemplo, pero sirve cualquier otro) que sea compatible con el Sistema de archivos del primero.
Por ejemplo, si el rootkit es ejecutado en un PC con Windows NT y el Sistema de Archivos utilizado es NTFS, deberemos iniciar el equipo con un S.O. distinto capaz de leer el sistema NTFS y podremos de esta forma examinar nuestro equipo en busca de archivos sospechosos.

Vamos un poco más allá, imagina que el rootkit no solo oculta directorios sino también cualquier proceso que empiece por _oculto_. En este caso podríamos subirle a la víctima cualquier programa, por ejemplo el r_admin.exe (tratado en el número 4 de PC PASO A PASO), lo renombraríamos a _oculto_radmin.exe y lo ejecutaríamos. En este caso, el archivo no se vería puesto que su nombre empieza por _oculto_, pero si hiciésemos un ctrl+alt+supr (para acceder al administrador de tareas) la tarea tampoco aparecería y para colmo, si hiciésemos un netstat tampoco veríamos el puerto de escucha de radmin.



Todo lo relacionado...

Todo lo relacionado con el "radmin", ctrl.+alt+supr (Administrador de Tareas de Windows) y netstat ha sido explicado en anteriores números.

- No me estarás tomando el pelo ¿no? (que ya soy mayorcito para creer en los Reyes Magos)

Te lo demostraré en este artículo. Tú mismo lo comprobarás en tu propio ordenador.

"... un rootkit es un código (programa) que al ser ejecutado en el ordenador-victima provocará una redirección y/o sustitución de binarios..."



Mucho cuidado!!!...

Mucho cuidado!!! Cuando experimentes con lo que te enseñaremos, hazlo en un equipo "de pruebas", no lo hagas en tu Sistema Principal. Ya te comentamos en el número 4 que, en cuanto te sea posible, consigas un PC para someterlo a tus prácticas :)

ROOTKITS: LA PESADILLA DE CUALQUIER ADMINISTRADOR

OCULTACIÓN DE PROCESOS. OCULTACIÓN DE DIRECTORIOS. OCULTACIÓN DE ARCHIVOS. OCULTACIÓN DE CONEXIONES.

PARTE II: LES PRESENTAMOS AL SR. NTROOT

1.- ¿Qué es el NTROOT?

Un rootkit se diseña (programa) para un Sistema Operativo en concreto, en este caso, os presentamos al SR. NTROOT. Por el nombre ya puedes imaginarte que es un rootkit para Windows NT.

Quizás encuentres el ejecutable (el *.exe) en algún sitio de Internet, pero normalmente los rootkits se "distribuyen" en forma de código fuente, es decir, que deberás compilar el programa para obtener un *.exe. Esto nos plantea un dilema moral... ... ¿qué hacemos? ¿te compilamos el código y lo ponemos en nuestra Web (www.hackxcrack.com) para que lo descargues o te enseñamos a compilarlo?

Decimos que es un dilema porque el que escribe este artículo se niega en rotundo a darte el *.exe y ya está, eso es atentar contra mi integridad moral, no quiero hacerlo, así de claro. Después de unos cuantos mails con el director de esta revista hemos llegado a un acuerdo: vamos a poneros el *.exe en la Web PERO también se te iniciará en el tema de la compilación (creo que en este número de PC PASO A PASO te enseñarán a compilar el netcat).



Nota del director:...

Nota del director:
El autor de este artículo nos ha planteado una situación que ya fue muy discutida cuando os compilamos el netcat con las opciones "interesantes" que explicamos en el número dos de esta publicación. En aquel momento no podíamos explicar cómo compilar un programa porque apenas acabábamos de empezar y la semilla de la curiosidad que estábamos plantando en tu interior ni siquiera había germinado, pero esta vez si que vamos a hacerlo. Teníamos pensado iniciar este tema cuando empezásemos los cursos de programación, pero después de mantener correspondencia con varios colaboradores me han convencido de que es el momento ideal para enfrentarnos a esto. Caso contrario, podemos caer en el error de "darlo todo" hecho, y eso no es bueno… además, necesitarás esta iniciación para cuando tratemos los exploits.

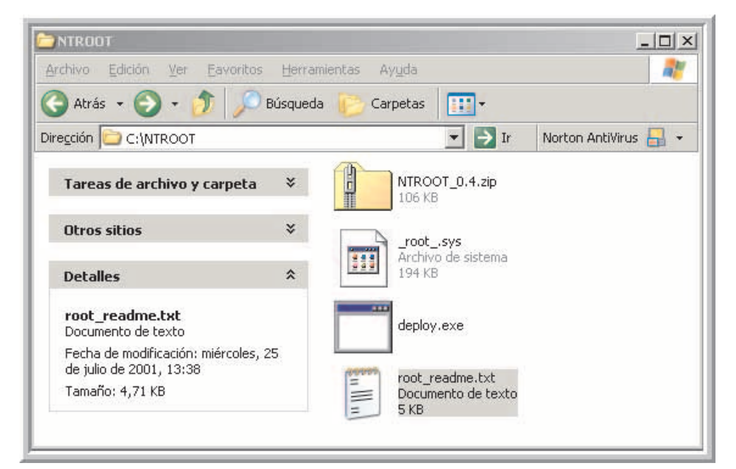
2.- Consiguiendo el NTROOT:

En nuestra Web (www.hackxcrack.com) encontrarás compilada la versión 0.4 del NT ROOTKIT, es decir, que podrás utilizarlo directamente. También te ponemos el código fuente de esta versión y de la versión 0.44 (versión no pública).

Venga, nos vamos a www.hackxcrack.com, sección programas y nos lo descargamos.

3.- Descomprimiendo:

Una vez tengamos el archivo NTROOT_0.4.zip en nuestro PC, procedemos a descomprimirlo. Nosotros hemos creado en nuestro PC la carpeta ntroot y hemos descomprimido allí el archivo.

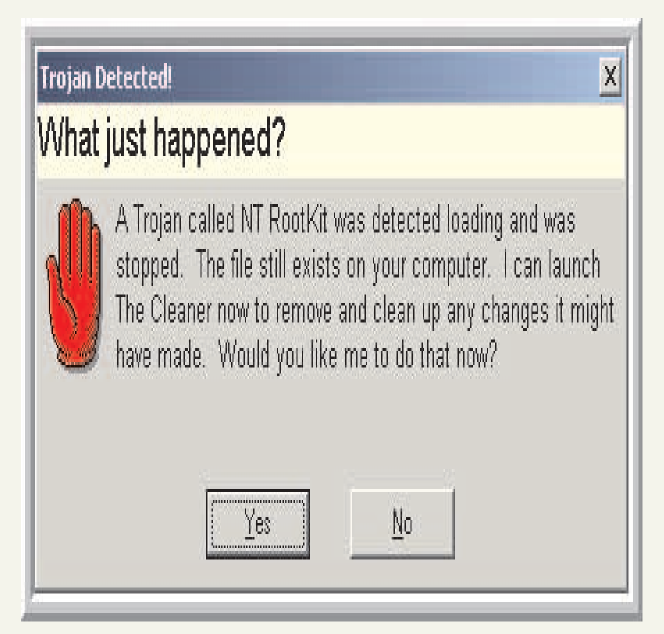


"...no debes pensar en que los rootkits son como los virus o troyanos. Los ROOTKITS son mucho más..."



Si tienes...

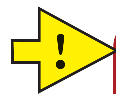
Si tienes el antivirus activado, debe empezar a cantar como loco y NO TE DEJARÁ DESCOMPRIMIRLO. Lo que tienes que hacer es desactivar el antivirus y descomprimir los dos archivos (lo mismo para algunos firewalls).



En este punto debemos comentar algo que creemos debes saber. Nosotros teníamos pensado dedicar la mitad de esta revista a explicar los ROOTKITS más conocidos, pero finalmente hemos decidido no hacerlo al igual que no solemos dedicar demasiadas páginas a los troyanos ampliamente difundidos (NET BUS, BACK ORIFICE, etc). El motivo es que los antivirus suelen detectar estos "bichos" a no ser que previamente neutralices los procesos correspondientes, algo que no hemos enseñado a hacer todavía.

A pesar de esto, no debes pensar en que los rootkits son como los virus o troyanos. Los ROOTKITS son mucho más, son considerados por quienes están metidos en el tema como verdaderas obras de arte dignas de las mentes más ágiles. Si tienes la suerte de conocer al creador (grupo de creadores) de algún rootkit y de que te lo "pasen", te aseguro que disfrutarás del código durante meses antes de que los antivirus sean capaces de detectarlos, puesto que su difusión suele ser más limitada :) Incluso os diré que suelen salir varias versiones de un mismo rootkit, una para su "difusión" y otra que solo tienen sus creadores con el código "modificado" para que no sea identificados por los antivirus.

4.- Ejecutando EL NTROOT



Avisamos...

Avisamos por última vez: la ejecución de cualquier rootkit puede provocar alteraciones en los binarios de tu Sistema Operativo y como puedes suponer las consecuencias son imprevisibles. Los ROOTKITS no son virus, este en particular podrás activarlo y desactivarlo cuando quieras, pero a pesar de todo, puede dejar secuelas en tu sistema. Te aconsejamos que realices las pruebas en un sistema "de pruebas".

Iniciamos una sesión por línea de comandos y nos vamos al directorio que contiene el rootkit, el c:\ntroot

c: (y pulsamos enter)
cd c:\ntroot (y pulsamos enter)

Hacemos un dir

dir (y pulsamos enter)

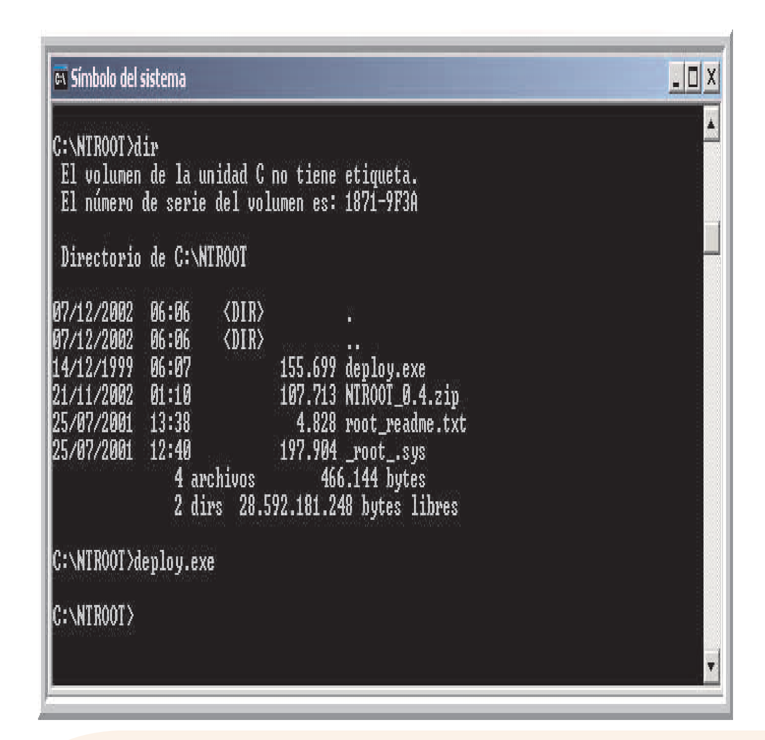


Ya hemos...

Ya hemos explicado hasta la saciedad eso de abrir una Ventana de comandos en anteriores números. Por sino sabes hacerlo, pásate por www.hackxcrack.com y en la sección de "portada y ampliación de contenidos" te lo explicamos.

Ahora instalamos (ejecutamos) el rootkit ejecutando el deploy.exe, ya sabes, simplemente escribe deploy.exe en la línea de comandos y pulsa enter.

deploy.exe (y pulsa enter)



Ya está!!! Ahora vamos a comprobar los efectos :)

5.- Efecto 1: Ocultación de Archivos y directorios.

Este rootkit, por defecto, oculta cualquier archivo o directorio que empiece por _root_ Venga, pon dir y pulsa enter... je, je... verás que ha desaparecido un archivo, el _root_.sys

No tengas reparos, vete al directorio raíz (el c:\) o cualquier otro. Crea un directorio con el nombre que quieras, por ejemplo noteveo. Mete dentro lo que quieras, por ejemplo 3GB de *.MP3 y finalmente renombra el nombre del directorio de noteveo a _root_noteveo. Ya está, directorio ocultado, ya tienes 3GB de información perfectamente ocultos... date cuenta que el contenido existe igualmente, todo lo que pongas en ese directorio puede ser ejecutado, descargado, copiado, etc. ¿Te das cuenta del poder que te ofrece este ROOTKIT?

Haz una prueba:
Vete al directorio raíz del sistema c:\
cd c:
Crea el directorio c:\hola
md c:\hola (y pulsa enter)
Mete dentro un archivo de texto, por ejemplo texto.txt
Hazlo con estilo, hombre, no me copies un archivo de texto a través del explorador de Windows. Para crear un archivo de texto llamado texto.txt en el directorio c:\hola con el contenido "He creado un txt desde la línea de comandos", simplemente tienes que poner:

echo He creado un txt desde la línea de comandos>c:\hola\texto.txt

Renombra el directorio hola a _root_hola

ren hola _root_hola



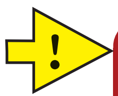
Haz un dir y verás que el directorio hola ha desaparecido.

dir

Si quieres haz un dir/a y verás que tampoco puedes verlo. Ya sabes que dir/a te permitirá ver los archivos/carpetas ocultos y de sistema, pero en este caso el directorio _root_hola ha sido ocultado por el rootkit, no por el sistema, por eso no puedes verlo ;)

Para poder ver tus archivos, solo tienes que acceder al directorio que has ocultado y del cual solo tú conoces el nombre y hacer un dir ;)

cd _root_hola (y pulsa enter)
dir (y pulsa enter)



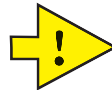
Ten en cuenta...

Ten en cuenta que puedes ver los archivos porque lo que has ocultado es el directorio (la ruta), si renombrases los archivos que contiene el directorio _root_hola poniéndoles el prefijo _root_ no podrías verlos. Si tu intención es montar un dump (explicado en anteriores números), con ocultar el directorio te sobra, podrás acceder a los archivos desde cualquier Cliente FTP con solo introducir la ruta que solo tu conoces ;)

6.- Efecto 2: Ocultación de Procesos.

Venga, un ejemplo sencillísimo, vamos a ocultar la calculadora de Windows ;)

- Busca en tu PC el archivo calc.exe.
- Cópialo donde quieras, por ejemplo en c:\
- Cámbiale el nombre por _root_calc.exe
- Por línea de comandos ejecuta c:\calc.exe
- Comprueba que el proceso es invisible abriendo el Administrador de tareas (teclas Ctrl+Alt+Supr) y buscando el proceso calc.exe.



No, no nos...

No, no nos hemos equivocado. Para ejecutar la calculadora hemos ejecutado calc.exe, no _root_calc.exe, así funciona este ROOTKIT. Cuando ocultas un ejecutable, para "iniciarlo" debes referirte a él con el nombre original, en este caso calc.exe. Si intentases ejecutar _root_calc.exe, no te funcionaría.



Ten en cuenta...

Ten en cuenta que la ocultación del proceso no implica la ocultación de las ventanas que pueda generar el programa ejecutado. Esto es ideal para esconder procesos, pero debes asegurarte de que los programas que ejecutes no te disparen pantallas de configuración y esas cosas.

Ahora espero que empieces a ver el motivo por el cual en PC PASO A PASO te hemos machacado tanto el tema de ejecución de programas en modo "silencioso", el serv-u, el radmin... (explicado en los números 1,2,3 y 4)

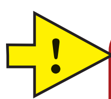
Ahora ya tienes una visión más amplia de lo que significa ocultar. Una cosa es ejecutar un programa de forma que no muestre pantallas (modo silencioso, lo que hemos estudiado hasta ahora), otra es ocultar el proceso mediante técnicas "de engaño" (llamar al proceso de otra forma, ampliamente tratado) y otra muy distinta es "hacer desaparecer" el proceso (lo que acabamos de hacer con el rootkit).

7.- Efecto 3: Ocultación de líneas del registro.

Esto ya es demasiado!!! Imagina que quieres hacer que un programa se ejecute de forma

automática cada vez que se reinicie Windows. De todos es conocida la clave del registro HKEY_LOCAL_MACHINE \Software \Microsoft \Windows \CurrentVersion \Run, es donde se ponen algunos de los programas que se inician con windows.

Solo tienes que añadir una nueva clave/valor que empiece por _root_ y desaparecerá de la vista del administrador, así de terrorífico.



Un día de...

Un día de estos te enseñaremos algunos "trucos" del registro para añadir claves sin que el sistema espere confirmación, describiremos las principales claves y esas cosas :)

8.- Otros efectos:

Están trabajando en conseguir otros "efectos", pero no están operativos al 100% por el momento y por eso no vale la pena que nos extendamos en su explicación. Por ejemplo la inclusión de un keylogger (para guardar en un fichero las teclas que pulsas de tu PC), un redirector de ejecutables que permita incluso saltarse las comprobaciones de CRC, acceso remoto al propio rootkit, etc.

9.- Activando y desactivando el NT ROOT

Finalmente, por si quieres activar/desactivar el NT ROOTKIT.

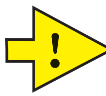
Activación: Introducir por línea de comandos la instrucción
net start _root_
Desactivación: Introducir por línea de comandos la instrucción
net stop _root_



No aconsejamos...

No aconsejamos la utilización de ROOTKITS porque:

- La mayoría son muy agresivos con el sistema "intervenido".
- Si el rootkit es ampliamente difundido no tarda en ser detectado por los antivirus, por lo que antes de ejecutarlos deberás anular/cerrar/modificar los procesos del antivirus "de turno", dejando al sistema "infectado" indefenso ante cualquier simple "agente infeccioso"... y eso no es bueno :(
- Normalmente requieren derechos de administrador para su ejecución.



Alerta!!!

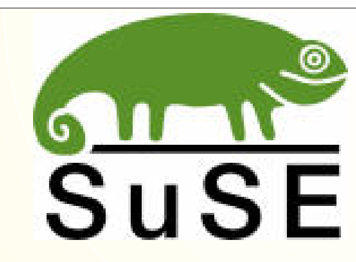
ALERTA!!!
El que escribe este texto advierte que la creación de un rootkit es muy compleja. Actualmente estoy trabajando junto a otras 6 personas en la creación de un rootkit para Windows XP que es capaz de crear un espacio de memoria "libre" al que acceder por un puerto (configurable) que es invisible ante cualquier visualizador de puertos (incluido el netcat). En 4 meses no hemos conseguido que funcione ni en el 20% de los equipos probados y por supuesto el código no está disponible para nadie.

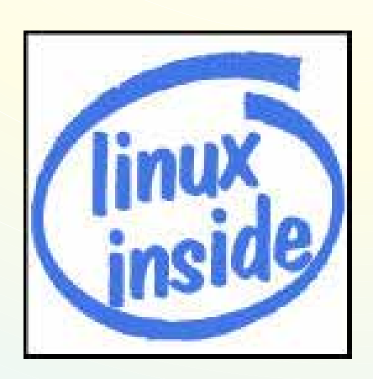
Diciendo esto debes pensar que soy un bocazas y que no tiene sentido publicarlo, si estoy trabajando en ello no le importa a nadie ¿verdad?. Pues lo digo por un motivo: El código de Windows es propiedad de Microsoft y no es de libre distribución, de hecho, ni siquiera puedes intentar husmear en él, es ILEGAL hacer ingeniería inversa y cualquier intento por averiguar su funcionamiento puede acabar con tu cuerpo en una celda. A pesar de todo, algunas personas han sido capaces de crear ROOTKITS para Windows realmente buenos… y ahora viene "la puntilla"… si un grupo de personas pueden crear rootkits para Windows que te impiden incluso ver los archivos que tienes en tu disco duro, señores y señoras, ¿quién impide a Microsoft

incluir "rootkits" en su código?

Piensa un poco, últimamente desde altas instancias del gobierno americano se está presionando para que se establezca algún sistema por el cual el FBI (o vete a saber quien) pueda en un momento determinado "entrar" en un sistema y ver los archivos contenidos. Según dicen es para nuestra seguridad (ya sabes, los terroristas), pero piensa que Microsoft, creadora del código de Windows, puede meterte un rootkit cuando quiera y te aseguro que su descubrimiento por parte de nosotros (simples mortales) sería prácticamente imposible. No creas que esto es un cuento, tengo información sobre la existencia de claves ocultas en el registro de Windows que podrían activar algún sistema de "escucha" en caso necesario. Si, si…. y la invasión extraterrestre está cerca ¿verdad?... piensa lo que quieras, búrlate si quieres, pero recuerda que quien crea el código es dueño y señor de su cometido!!!

P.D. Nadie me ha traído un extraterrestre a casa para hablar con él, pero sí me han traído a casa "rootkits" cuyos efectos harían palidecer al administrador más pintado… quedamos todos advertidos. Que te metan un rootkit es un problema, pero que te vendan un sistema operativo "rootkiteado" de fábrica, eso no tieme nombre!!!





WAREZ: APPZ, GAMEZ, MPZ, DIVX, FTPZ, 0-DAY



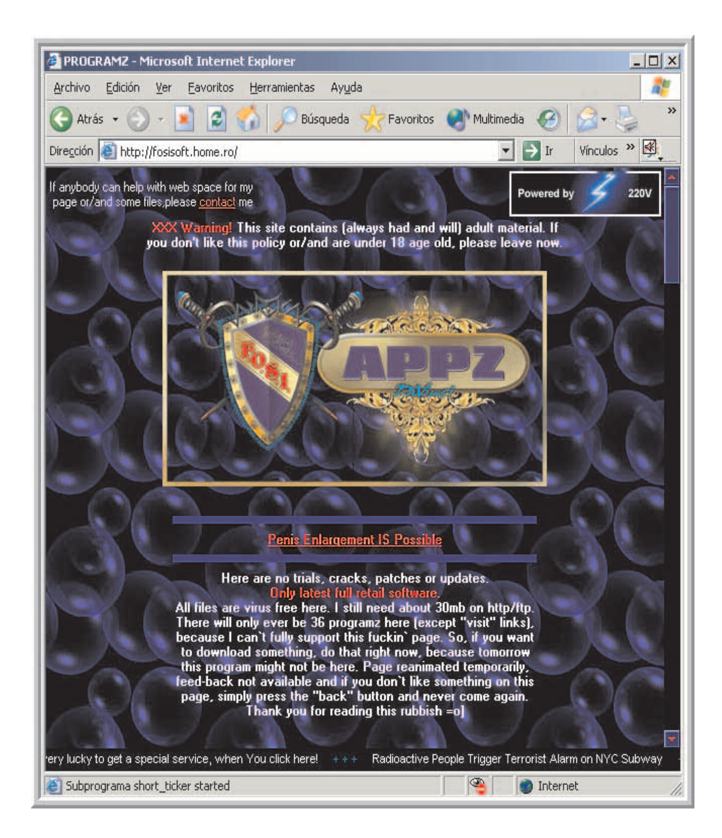
A TODOS NOS HA PASADO!!!

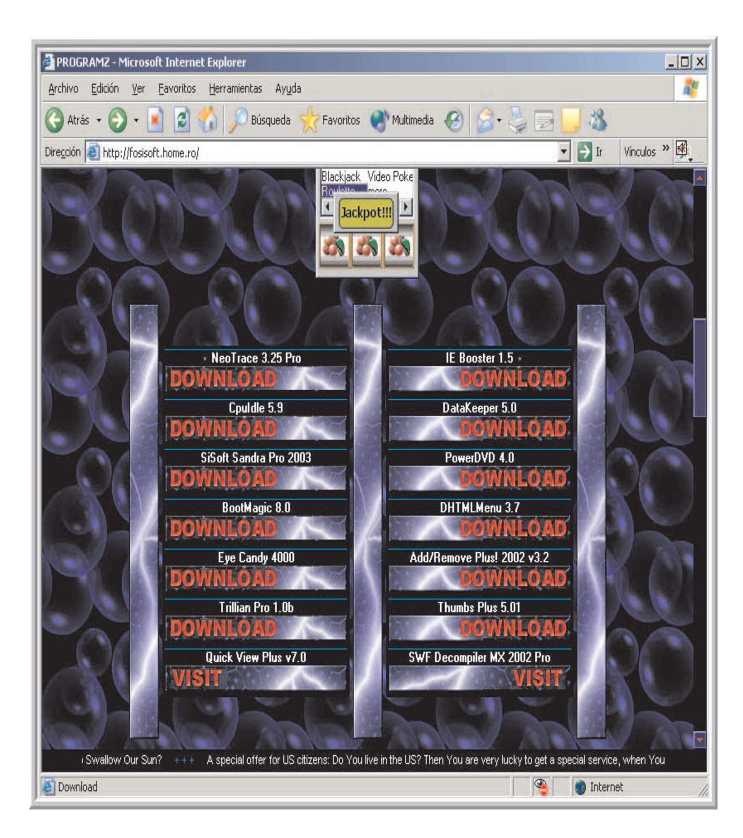
Vamos a ver si de una vez por todas acabamos con esto. Si quieres un programa por el motivo que sea y no tienes dinero para comprarlo, lo que tienes que hacer es ir a la página Web de ese programa, descargarte una versión de prueba (trial) y disfrutar de él durante unos días. Si pasados unos días deseas seguir disfrutando de ese programa, no te queda más remedio que iniciar la búsqueda por Internet.

1.- Al principio de los tiempos, hace muy poquito...

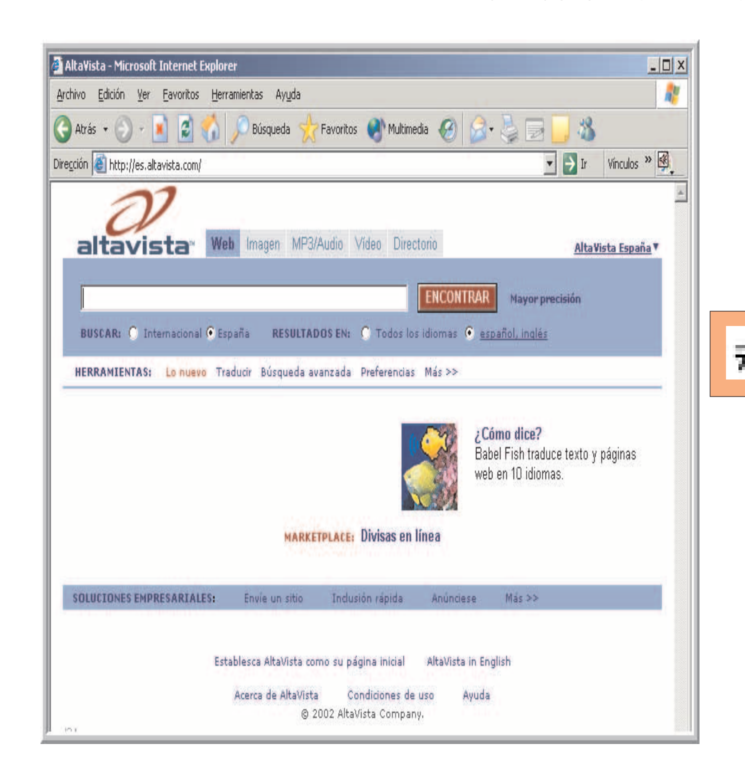
Imagina que estabas buscando una utilidad llamada Nero que quema CDs que da gusto. En aquellos felices tiempos, cuando eras un "novatillo", se te ocurría la idea de ir a los buscadores de toda la vida (como www.altavista.com) y poner NERO APPZ. Lo más seguro es que acabases navegando entre páginas porno inglesas donde aparentemente hay cientos de descargas de programas gratis pero que en realidad, después de navegar durante un par de horas y luchar contra todo tipo de POP-UPS, finalizabas tu trayecto sin encontrar nada y reiniciando un PC cargadito de cookies y demás molestos bichos. Al principio esto nos ha pasado a todos, había que tomárselo con filosofía.

Pasados unos días y después de mucho buscar, aprendías que GOOGLE (www.google.com) era el mejor buscador de Internet, empezabas a encontrar páginas de descarga interesantes (las famosas y eternas fosi, www.fosi.da.ru)

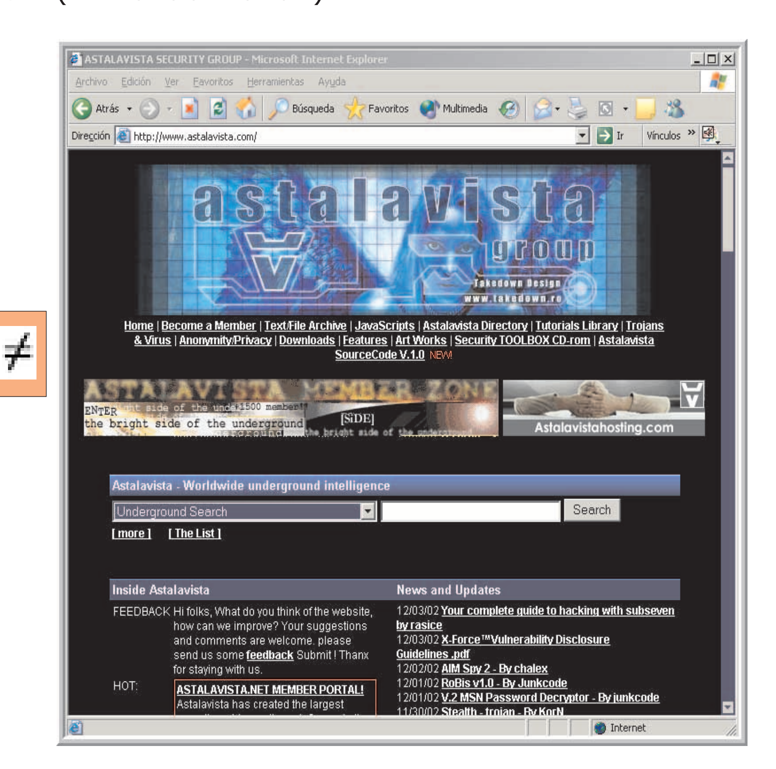




Y descubrías ASTALAVISTA (www.astalavista.com).



≠



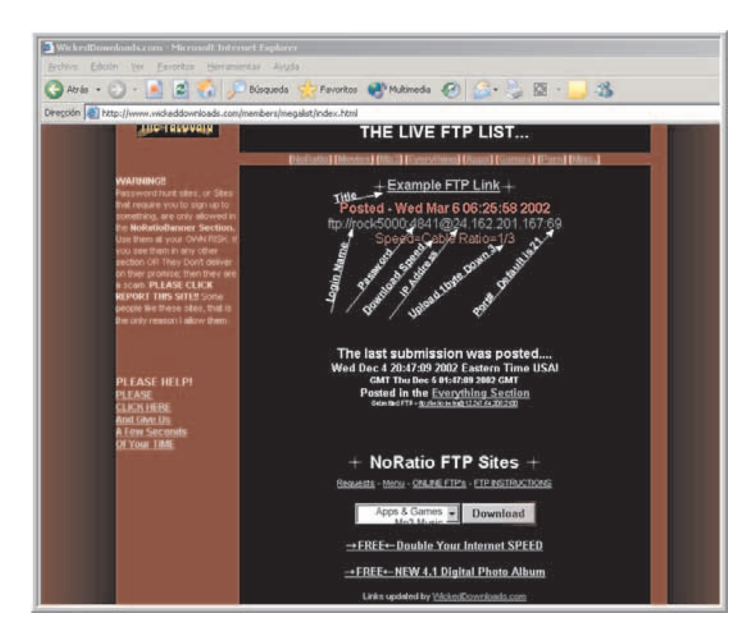

www.altavista.com

www.astalavista.com

Mas tarde y después de un par de sesiones en el hispano (CHAT) acababas enterándote de que el Warez ("cosas gratis") se movían a través de unas cosas llamadas Servidores FTP y que lo más interesante eran las 0-DAYS (aplicaciones craqueadas recién salidas del horno). Así que ni corto ni perezoso llegabas a páginas como http://www.wickeddownloads.com/ donde balbuceando el poco ingles que te habían enseñado conseguías instalar en tu equipo un Cliente FTP y con mucho esfuerzo entrabas a los Servidores FTPs que una gente muy rara que sabía mucho más que tu había montado.

viste tu FTP lleno de IPs pululando por el servidor, que sensación de DIOS tenías cuando jugueteabas con tantas personas haciéndo todo tipo de travesuras ;p.

El tiempo pasaba y nuevamente llegaba el aburrimiento, por lo que decidías meterte en uno de esos grupos Warez de FTPs de quien tanto habías oído hablar (www.hardextreme.org). Después de demostrar tus conocimientos te admitían en uno y vislumbrabas un nuevo mundo ansioso de ser descubierto (en aquella época, en perfecto inglés, claro).



Ahhhh, que días aquellos, que gran victoria era cada Servidor FTP conquistado y cada programa "pillado". Eras un pequeño Dios, una insignificante mente curioseando por los confines de un mundo vedado para la mayoría. Al cabo de un tiempo, uno se cansaba de visitar FTPs y decidía montar su propio Servidor FTP. Que emoción!!! Después de descubrir los programas capaces de crear tales artilugios y de pelearte con cientos de conceptos desconocidos conseguías montar en tu PC un Servidor FTP y ponerlo en una lista para que te entrase quien quisiese y pillase tus archivos. Ummm, qué sensación tan fantástica la primera vez que

A base de traductores y horas y horas de prácticas descubrías que esa gente tan rara e inteligente (desde la vista de un pobre ignorante) lo que hacía es escanear la red buscando Servidores FTP de empresas con errores de seguridad. El error buscado no era mas que encontrar Servidores FTPs de acceso anónimo (no protegidos por contraseña) y con algún directorio escribible, es decir, un sitio donde poder subir programas. Utilizando escaneadores encontrabas esos Servidores FTP y con un Cliente FTP subías los programas y anunciabas al resto de la peña tu conquista para que pudiesen bajarse el "material" que habías subido

con terrible esfuerzo. De verdad que se aprende rápido, no pasaba un solo día sin encontrar servidores "susceptibles" de ser conquistados, y aprendías que habían directorios especiales donde no podías subir nada porque estaba denegado el derecho de escritura, y aprendías a ocultar el material subido de los ojos de la gente, y aprendías a crear directorios ocultos y solo "escribibles" por ti, y llegaba un día en que conocías todos los tipos de Servidores FTP y sus vulnerabilidades.

Aquí se abría una nueva puerta, porque las vulnerabilidades te permitían salir del Servidor FTP y aparecer en Servidor Principal, es decir, acceder al resto del disco duro del Servidor Hackeado. Recuerdo con nostalgia la primera vez que conseguí una shell de sistema a través de una escalada de directorios, allí estaba yo, frente a un Servidor, cara a cara ante lo desconocido… el resto ya te lo puedes imaginar, poco a poco y día a día, con mucho esfuerzo y muchas horas de lectura inglesa acabas conociendo todo tipo de Servidores que corren todo tipo de Servicios y cada uno de esos servicios era una nueva puerta que abría un nuevo horizonte lleno de posibilidades.

Al cabo de los meses y de los años, sin darte cuenta, la gente empieza a preguntarte cosas que tu sabes responder. Realmente no te has dado cuenta del cambio que ha habido en tu interior, ahora tú eres quien responde y se dispara un flash en tu mente que te hace recordar, recordar un pasado cercano en el que TÚ eras quien preguntaba. Entonces te das cuenta por primera vez del largo camino recorrido, hablas con familiaridad de conceptos que otros apenas saben pronunciar y una vez más te sorprendes al verte reflejado en quienes ahora te preguntan. Muchos se habían quedado enganchados con las descargas llenas de virus y pornografía, otros en los chats con los "chat-servers", otros con los Clientes FTP (nunca se atrevieron a montar el suyo propio), otros se quedaron anclados montando Servidores, algunos entraron en grupos de FTP pero nunca supieron cómo escalar directorios y unos pocos, muy pocos, acabaron como yo, enganchado en el fantástico mundo del hacking, estudiando RFCs, montando servidores de todo tipo, probando versiones de todo tipo de S.O. y disfrutando de cada nuevo reto.

Señores, así eran las cosas antes, cuando no existía el P2P!!!

2.- En los tiempos actuales… adiós al romanticismo.

Toda esta parrafada es para que dejes de enviarnos mails preguntando dónde conseguir tal o cual programa, que no, que PC PASO A PASO (Los cuadernos de Hack x Crack) no te lo va a decir. Ahora es tan sencillo conseguir cualquier cosa que busques, es tan ridículamente sencillo y el esfuerzo que debes hacer es tan ínfimo que es una verdadera tontería que nos envíes un mail preguntando por tal o cual programa o por tal o cual crack.

No te enfades si no te contestamos ese tipo de mails, por favor, si quieres un programa visita la página de cualquier P2P y simplemente cógelo tu mismo. Por si no sabes de que hablo (cosa que me extrañaría), empieza por el e-donkey, un clásico entre los clásicos, si es que se puede denominar clásico a un evento desarrollado en los últimos dos años, claro.

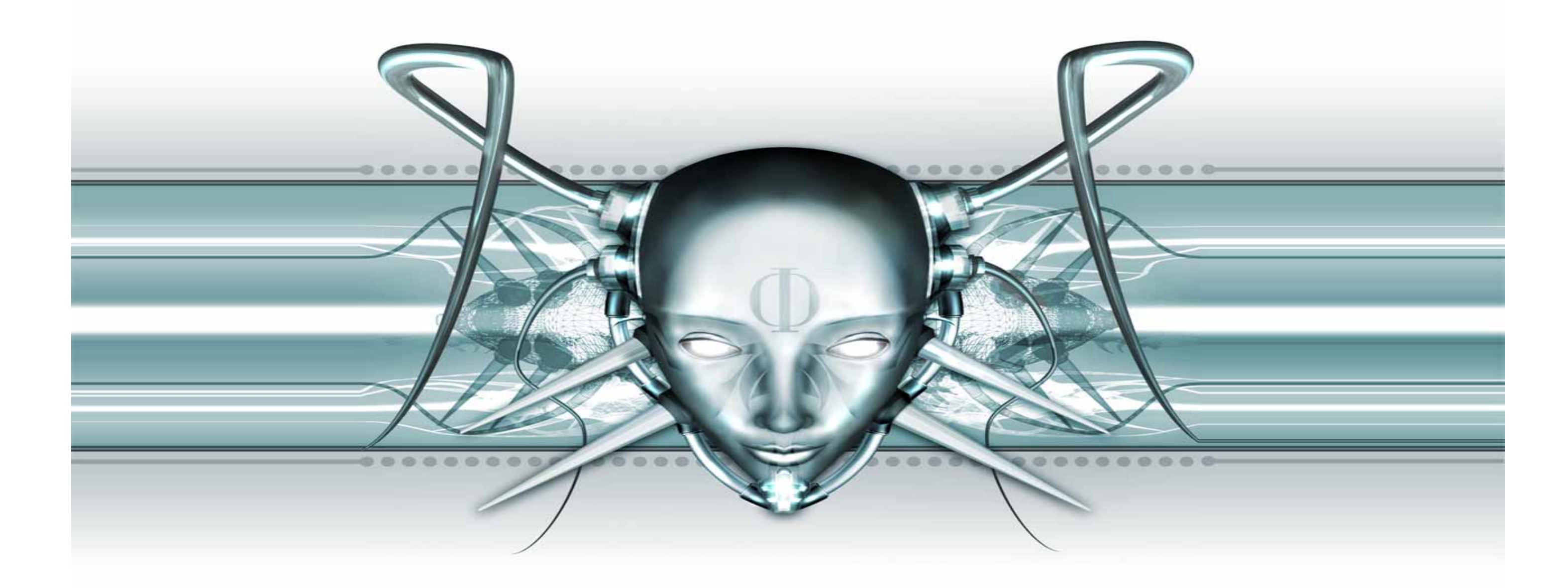
Para conseguir gratis lo que quieras solo tienes que ir a www.edonkey2000.com, bajarte el edonkey, instalarlo y visitar una de las numerosas comunidades españolas de la red edonkey, por ejemplo www.spanishare.com. Se acabó, ya tienes todo lo que quieras y sin esfuerzo.



3.- La intención de este artículo.

- Que no nos pidas más programas por mail.
- Informarte de que nosotros no "movemos" WAREZ.
- Que si quieres un programa, solo tienes que mover un dedo (y a veces ni eso)
- Y en último lugar, explicarte el camino que antes recorría alguien que quería lo que tu ahora obtienes sin esfuerzo. Por eso quiero que comprendas una cosa, pedir un programa hoy en día es casi una falta de respeto, lo tienes tan a mano que pedirlo es como pedir que te mastiquen la comida y te la pongan en la boca. Por favor, si quieres algo --> edonkey2000

En este número de PC PASO A PASO se han vertido opiniones sobre la piratería, opiniones que han servido de antesala a este texto. Ya sabes lo que pensamos de la piratería, así que la "misión" de este texto NO ES incitarte a delinquir en forma alguna. Las redes P2P son una realidad y están a tu disposición, solo tú decides cómo utilizar el material que te descargues.



APRENDIENDO A COMPILAR PROGRAMAS

COMPILA TU PROPIO NETCAT

1.- Presentación.

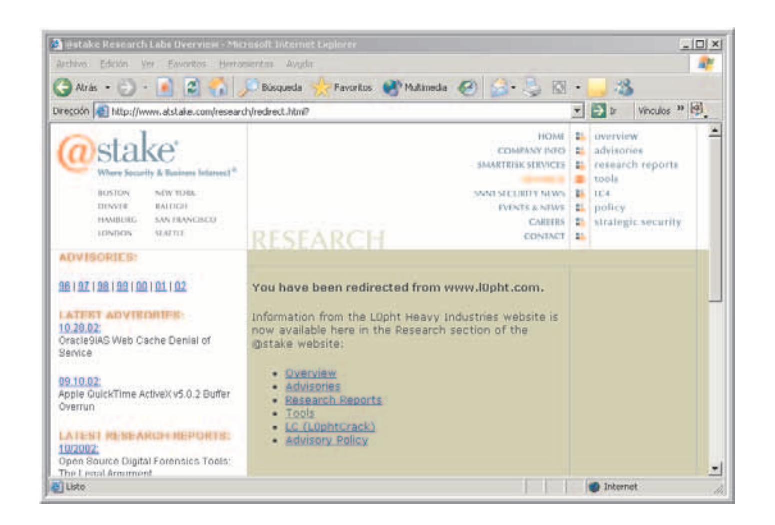
Si nunca te has enfrentado al proceso de compilación del código de un programa, HA LLEGADO MOMENTO!!! Compilar no es difícil, pero si nunca lo has intentado, al principio te parecerá un poco complicado. Aquí estamos nosotros para intentar iniciarte un poco en el tema, que no es para tanto :)

En este artículo vamos a compilar el NETCAT PARA WINDOWS. Para quien no lo sepa, el netcat es un mito, una herramienta que puede hacer "casi de todo" en La Red, es como una caja de herramientas ;)

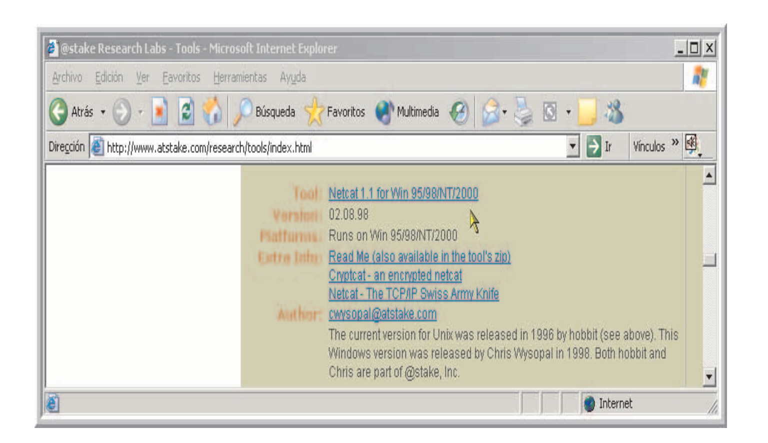
El netcat puede compilarse "tal cual" o añadiendo un par de opciones que activarán unas utilidades "extra" que nos permitirán hacer "cositas interesantes", como ya experimentamos en el número 3 de PC PASO A PASO (Los cuadernos de Hack x Crack). Nosotros lo compilaremos añadiendo esas opciones "interesantes", para que luego no digas ;)

2.- ¿Qué necesitamos?

Lo primero que necesitamos es el código fuente del NETCAT. Puedes descargarlo de http://www.l0pht.com/ la cual nos redireccionará a http://www.atstake.com/research/redirect.html? (ver imagen)



En el centro (mas o menos) veremos el enlace TOOLS, lo pulsamos y nos aparecerá una página en la que encontrarás el NETCAT (sección 3: Network Utility Tools). Bájate la versión para Windows :)





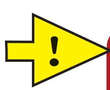
El netcat ...

El netcat puedes descargarlo también de nuestra Web (www.hackxcrack.com), tanto el código fuente como el programa ya compilado :)

COMPILACION DEL NETCAT

Lo segundo que necesitamos es el **Visual Studio 6** o el **Visual .NET** (el compilador), nosotros seguiremos esta práctica con el **Visual Studio 6**. Vamos a ser muy claros, tarde o temprano, por un motivo u otro necesitarás este programa, si, si, ya se que podemos hacer lo mismo con otros, pero no podemos negar la realidad... debes tener una copia del **Visual Studio** siempre preparada para "las urgencias" ;)

Como es un programa "de pago", tendrás que buscar y utilizar una versión de prueba o descargar una "copia de seguridad" con el edonkey o cualquier otro P2P. Si te instalas el edonkey (encontrarás más información en esta misma revista) y haces una búsqueda (search) por el nombre "visual Studio", encontrarás disponible el archivo llamado "Microsoft.Visual.Studio.6.0.(Visual.Basic.y.C).[1.solo.CD..serial]_[nero.iso.nrg]_[español.spanish.castellano]_[by.HARETZ].raR". Pues venga descargatelo, descomprímelo con Winzip o Winrar y obtendrás el archivo "Microsoft Visual Studio 6.nrg".



Para quien no ...

Para quien no lo sepa, un archivo con la extensión nrg es una imagen de CD realizada con el Nero Burning Rom. Por lo tanto deberás "quemar" la imagen, es decir, utilizar el Nero para grabar un CD.

Si no tienes grabadora de CDs, no te preocupes, aquí tenemos soluciones para todos ;p. Puedes ir a http://www.daemon-tools.com/ y descargate las Daemon Tools (actualmente en su versión 3.26). Este programa te permite "ejecutar" (leer) directamente una imagen de CD; pero las Daemon Tools no pueden leer directamente imágenes de CD con la extensión *.nrg (del nero), por lo que deberás transformar el Visual Studio 6.nrg en Visual Studio 6.iso (iso es un Standard de imágenes de CD). No extensión directamente ;p

Para hacer esta transformación necesitarás el programa Winiso, que lo encontrarás en http://www.winiso.com/. Este programa te permite, entre otras cosas, transformar imágenes *.nrg en *.iso (Menú Convertir --> Conversor para otros formatos).

Una vez obtenido el archivo Visual Studio 6.iso, lo cargamos con las Daemon Tools y te aparecerá la ventana de instalación del Visual Studio 6.

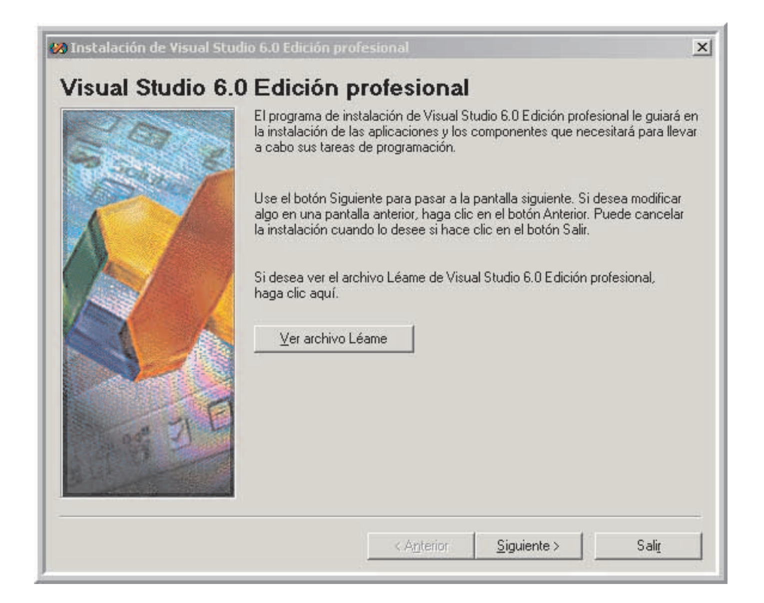
APUNTE 1: Si necesitases la versión completa del Winiso, ya sabes, edonkey ;)

APUNTE: Si nunca has realizado este proceso, admitámoslo, no estás muy ducho en esto de descargarte "programitas" de Internet. Actualmente, cualquier copia de seguridad que te descargues de Internet precisa de esta "manipulación" (y otras) para conseguir iniciar el proceso de instalación. Si realmente no tienes ni idea de lo que te acabamos de explicar, envía un mail a director@hackxcrack.com con el asunto "Quiero un artículo sobre las Daemon Tools" y según los mails recibidos el director pondrá en el número 6 de PC PASO A PASO un artículo que explique en profundidad el tema :)

3.- Instalando el Visual Studio 6

Ha llegado el momento. Iniciamos la instalación del Visual Studio 6 introduciendo el CD previamente "quemado" con el Nero o cargamos la imagen Visual Studio 6.iso con el las Daemon Tools y nos aparecerá la ventana de instalación :)

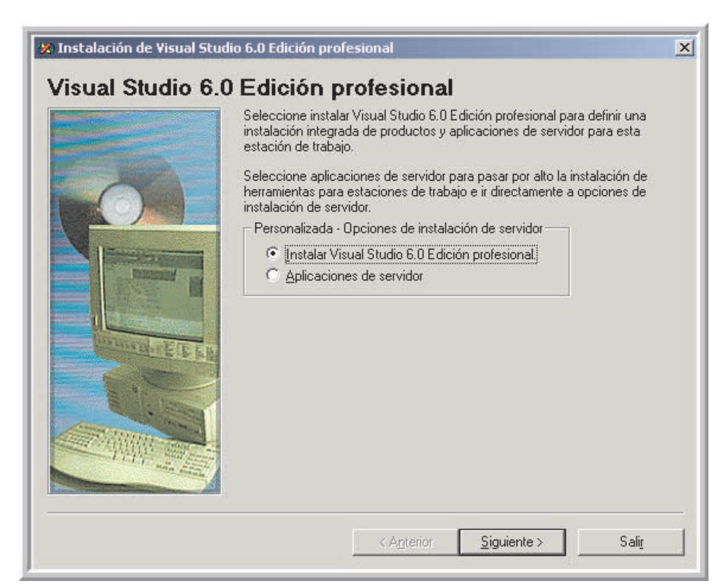
 COMPILACION DEL NETCAT



Pulsamos siguiente y nos aparecerá una ventana donde seleccionaremos Acepto el Contrato y pulsaremos siguiente. Nos aparecerá otra ventana donde se nos pide un código, ningún problema, si te has descargado la copia de seguridad del e-donkey, al descomprimir te sale el código en un archivo de texto ;)



Pues eso, lo introduces, pulsas siguiente y en la ventana que te aparecerá a continuación seleccionas Instalar Visual Studio 6.0 Edición Profesional.





Esta última ...

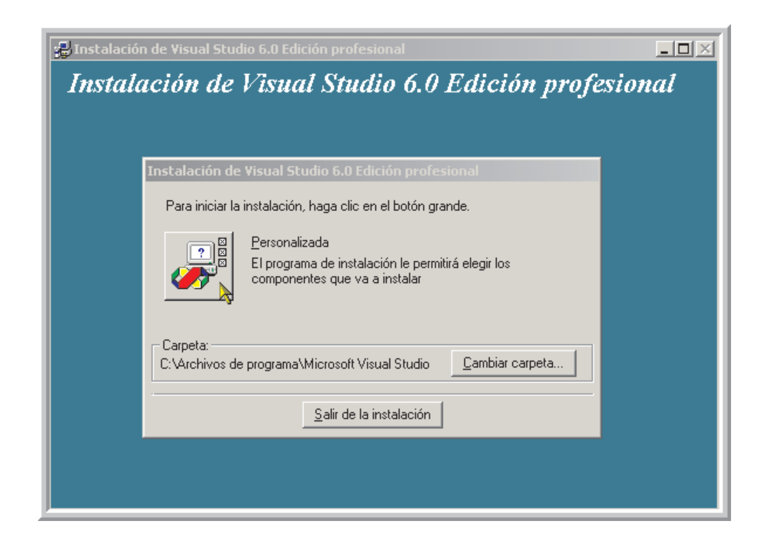
Esta última ventanita será distinta en función del Windows utilizado. La primera opción es la que debes seleccionar, la que te hemos descrito antes de la imagen, la segunda (Aplicaciones de Servidor) te instalaría una serie de "extras" que por el momento no son necesarios.

Pulsamos siguiente y nos aparecerá una ventana donde nos pregunta la ruta de instalación, mejor no la cambiamos (por si las moscas ;p) y pulsamos siguiente, con lo que se iniciará la instalación.

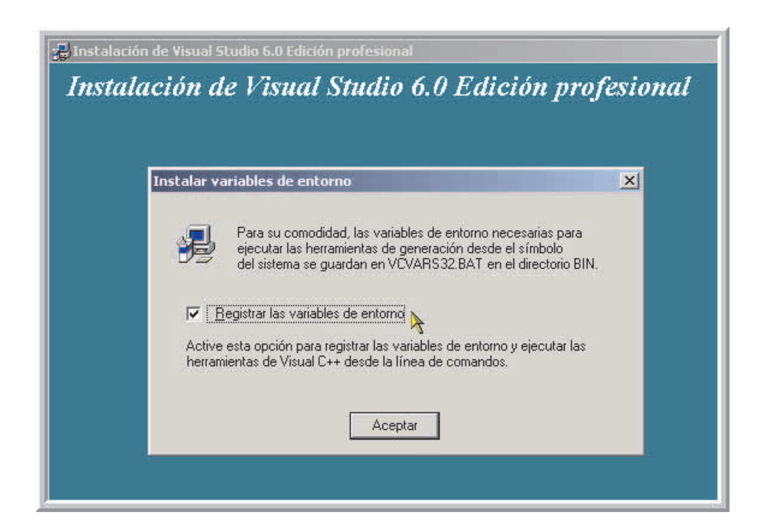
Quizás te aparezca una ventana pidiendo que cierres todos los programas para poder proseguir, pues ya sabes, cierra todo lo que tengas abierto y confirma.

Llegarás a una ventana como la de la imagen, simplemente pulsa sobre el botón grande tal y como te indican.

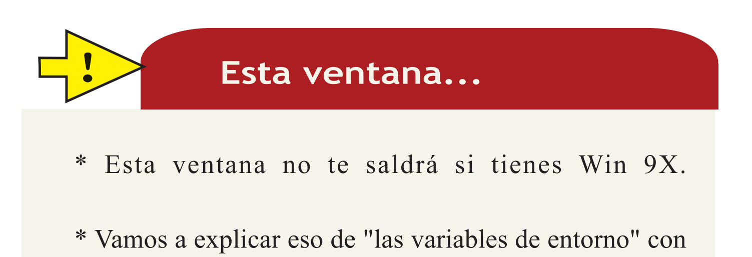
COMPILACION DEL NETCAT



En la siguiente ventana te permiten seleccionar los componentes que deseas instalar, venga no seas rácano, ya que nos hemos metido en el "lío" pulsamos sobre el botón Seleccionar Todo (a la derecha) y después pulsamos Continuar, con lo que llegaremos a una ventanita MUY IMPORTANTE.



Seleccionaremos la opción Registrar variables de Entorno y pulsaremos aceptar.



Esta ventana...

* Esta ventana no te saldrá si tienes Win 9X.

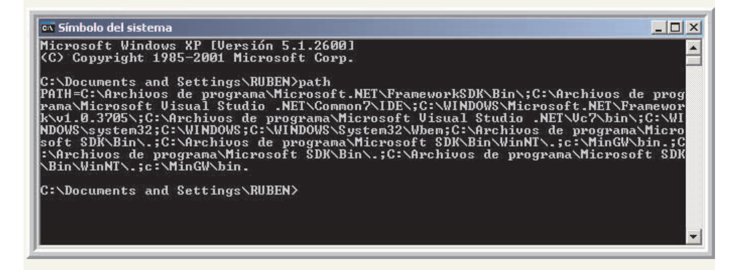
* Vamos a explicar eso de "las variables de entorno" con ejemplo que ya conocemos:

Cuando abrimos una ventana de comandos, nos encontramos por defecto en un directorio, en el caso de la imagen c:\Document and Settings\RUBEN\.



En principio, solo podríamos iniciar los ejecutables que estuviesen en ese directorio (carpeta), pero ya sabes que si pusiésemos, por ejemplo, netstat -a-r, se ejecutaría el programa netstat. Si hacemos un dir, veremos que el comando netstat no está en esa ruta… ummm… ¿por qué podemos entonces ejecutarlo?

Para que puedas ejecutar un programa por línea de comando desde cualquier directorio, debes decirle al sistema dónde está ese archivo que deseas ejecutar proporcionándole una "ruta". Si introduces el comando path y pulsas enter, verás algo parecido a esto (posiblemente mucho menos ;))



Fíjate bien, son directorios, y cualquier programa que esté dentro de esos directorios puede ser ejecutado desde la línea de comandos sin necesidad de entrar en la carpeta que alberga el programa.

Imagina que creas un directorio llamado utilidades en el disco c: y quieres que cualquier programa que metas en ese directorio pueda ser ejecutado desde cualquier sitio. Simplemente tendrías que añadir esa ruta al path del sistema, es decir, deberías introducir por línea de comandos

COMPILACION DEL NETCAT

path c:\utilidades;%path% (y pulsar enter)

Fíjate bien que detrás del directorio debemos poner un punto y coma y OJO!!!, detrás del punto y coma debemos poner %path%. Si te olvidas de poner %path% borrarás el path original y te quedarás solo con el que acabas de introducir, con lo que el sistema posiblemente dejará de funcionar correctamente.

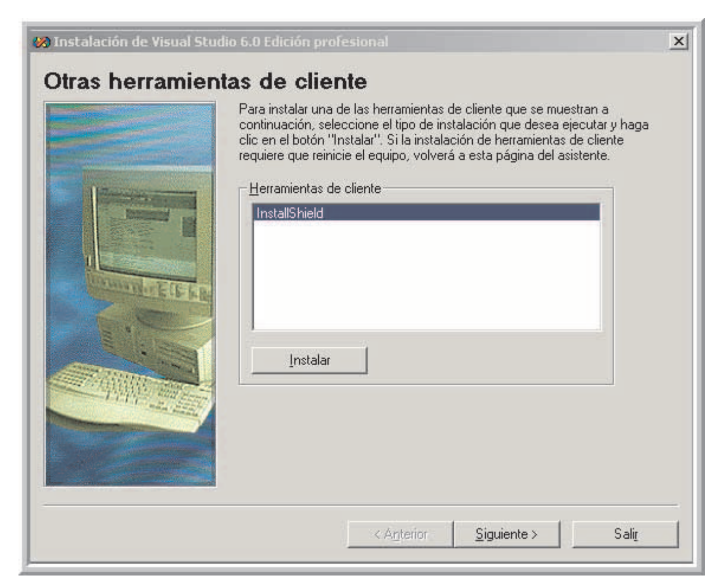
Finalmente nos aparecerá esta pantalla (no le hagas ni caso).



pulsaremos aceptar y finalizará la instalación del Visual Studio C++ dando paso posteriormente a la instalación del MSDN --Microsoft Developer Network Library -- (documentación y ejemplos).
-- excepto en XP, te pedirá que reinicies. Una vez reiniciado la instalación continuará por este paso --



Le diremos que no picando en Instalar MSDN y enter. Después te pedirá si quieres instalar el InstallShield, selecciónalo, pulsa Instalar y acepta todos los valores por defecto. Cuando acabe te volverá a aparecer la misma ventana invitándote a instalar de nuevo el InstallShield



Pero como ya lo hemos instalado en lugar de pulsar el botón instalar pulsaremos el botón siguiente y en la siguiente ventana de nuevo pulsaremos siguiente, y finalmente nos aparecerá otra ventana donde se nos pedirá que nos registremos. Simplemente deseleccionaremos la opción y pulsaremos finalizar.



Si durante la Instalación tienes dudas, ya que nos hemos metido en el tema, opta siempre por instalarlo todo. Si sigues los pasos que te hemos mostrado, tendrás una instalación mucho más completa de lo que necesitamos para compilar el NETCAT, pero mejor que sobre y no que falte :)

4.- Ejecutando el Visual Basic 6:

Ejecuta el Microsoft Visual C++ 6.0 mediante

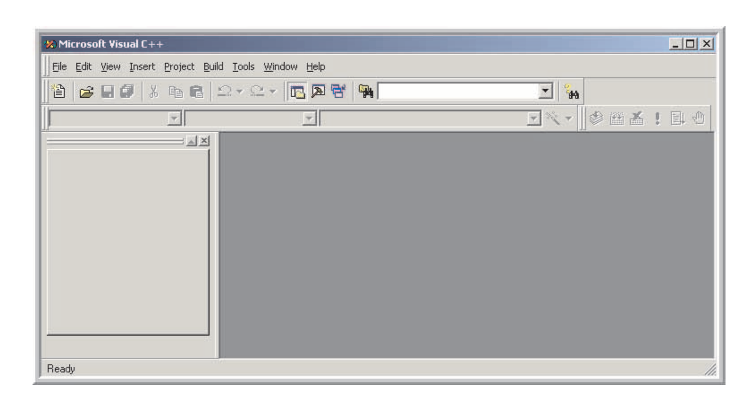
 COMPILACION DEL NETCAT

el Menú Inicio de la Barra de Tareas del Windows --> Microsoft Visual Studio 6 --> Microsoft Visual C++ 6.0



si, si, ya se que mi equipo está muy cargadito de programas ;)

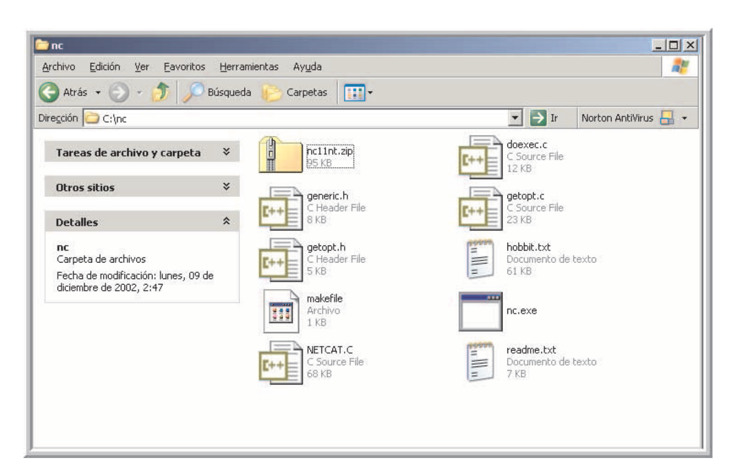
Y finalmente aparecerá ante ti la interfaz del Visual Studio C++ 6.0



Se acabó, ya estás frente a la interfaz gráfica del programa.

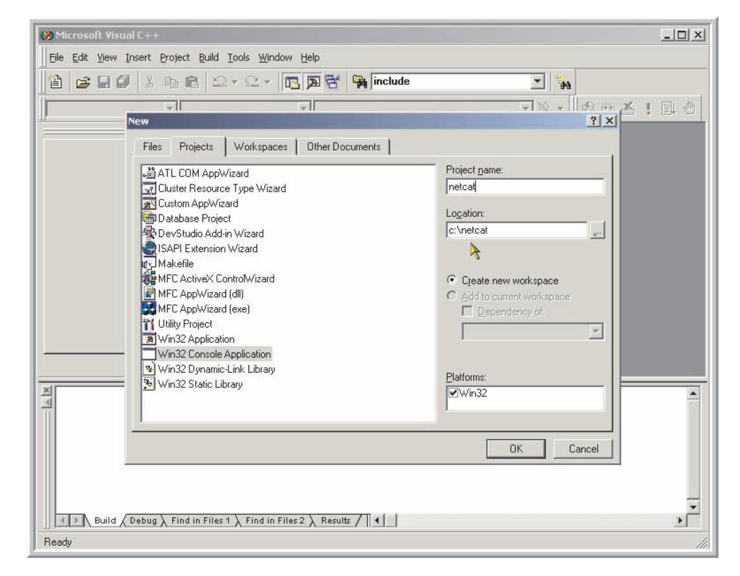
5.- Creando el Proyecto NETCAT.

Dejamos un momento el Visual C++ y creamos una carpeta en nuestra unidad c: llamada nc y descomprimimos dentro el netcat que nos hemos agenciado en http://www.l0pht.com/ (el archivo nc11nt.zip), con lo que obtendremos este resultado (los archivos que hemos descomprimido son el código fuente del netcat y los utilizaremos para obtener el ejecutable netcat.exe).



Crea otra carpeta en el disco c: llamada netcat y déjala vacía. Aquí es donde aparecerá el netcat.exe compilado por nosotros :)

Ahora volvemos al Visual C++ y creamos un nuevo proyecto: Menú File --> News y nos aparecerá una ventana. Selecciona la pestaña Projects.



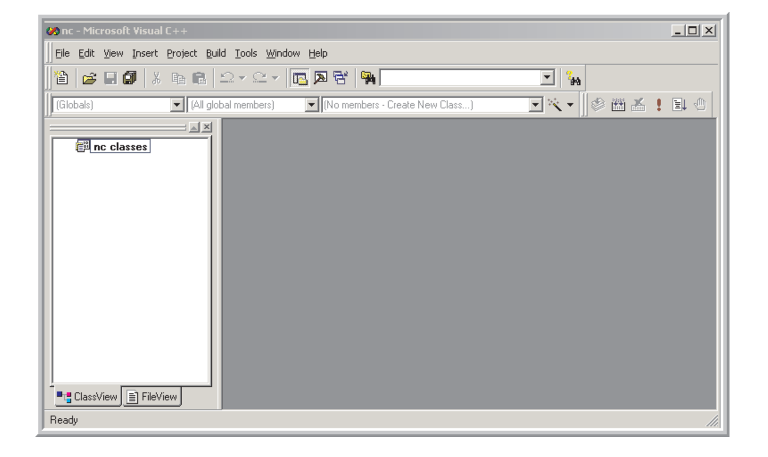
En la ventana Projects tienes una lista de "tipos de proyecto".

- selecciona Win32 Console Application. Esto te permitirá crear un programa tipo consola, es decir, que podrás ejecutar y "relacionarte" (pasarle comandos) con el programa por línea de comandos.

- a la derecha, en Project Name, escribe netcat y el apartado Location debería autocompletarse

COMPILACION DEL NETCAT

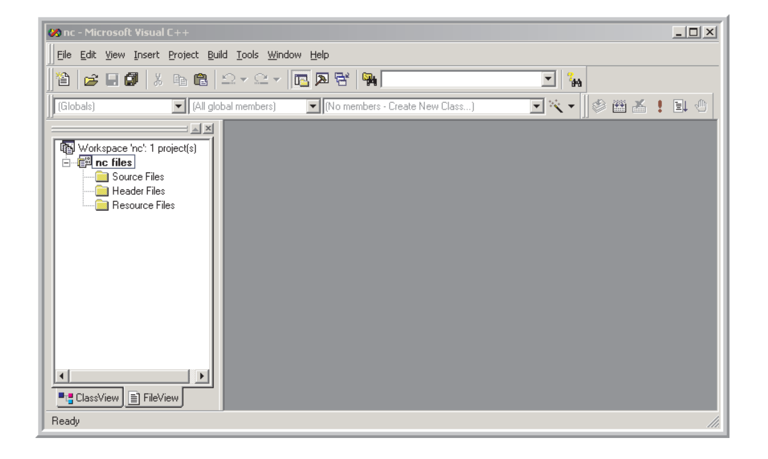
Pulsa OK y en la siguiente ventana selecciona empty project y pulsa Finish, en la siguiente ventana OK y nos encontraremos de nuevo ante la ventana principal del Visual C++



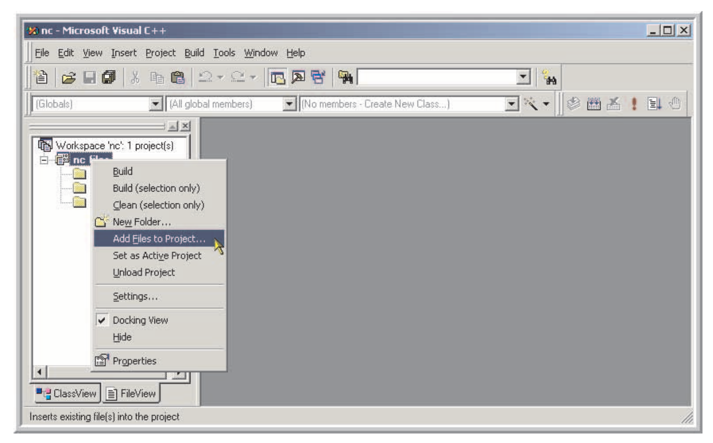
6.- Añadiendo archivos al proyecto.

Ahora vamos a proporcionarle al Visual Studio el código del programa.

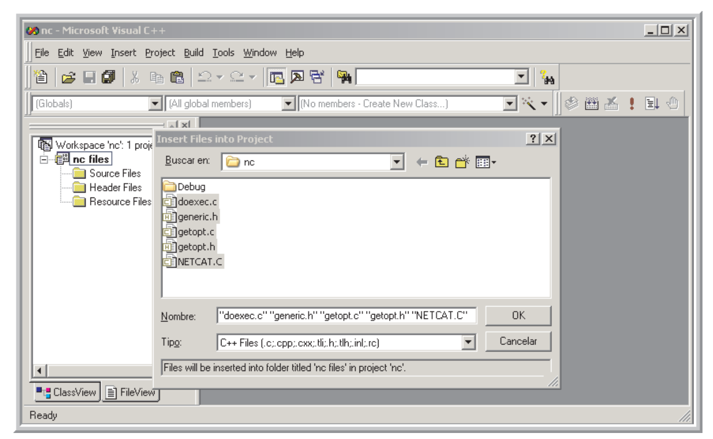
Fíjate bien abajo en la izquierda. Puedes ver dos pestañas: Class View y File View. Selecciona la segunda (File View) y obtendrás lo siguiente



Ahora puedes ver que en el cuadro blanco de la izquierda, arriba, tienes en negrita nc files. Pon el ratón sobre nc files, pulsa el botón derecho y selecciona Add Files to Project (añadir archivos al proyecto).



Aparecerá una ventana que te permitirá buscar en tu disco duro los archivos que desees añadir al proyecto. Tienes que ir a c:\nc (recuerda que es donde pusimos el código fuente). Una vez allí selecciona los cinco archivos que tienen la extensión C y H (doexec.c, generic.h, getopt.c, getopt y NETCAT.C)



Y pulsa OK.



Para seleccionar varios archivos mantén pulsada Ctrl mientras con el Mouse pulsas sobre los archivos que deseas marcar.

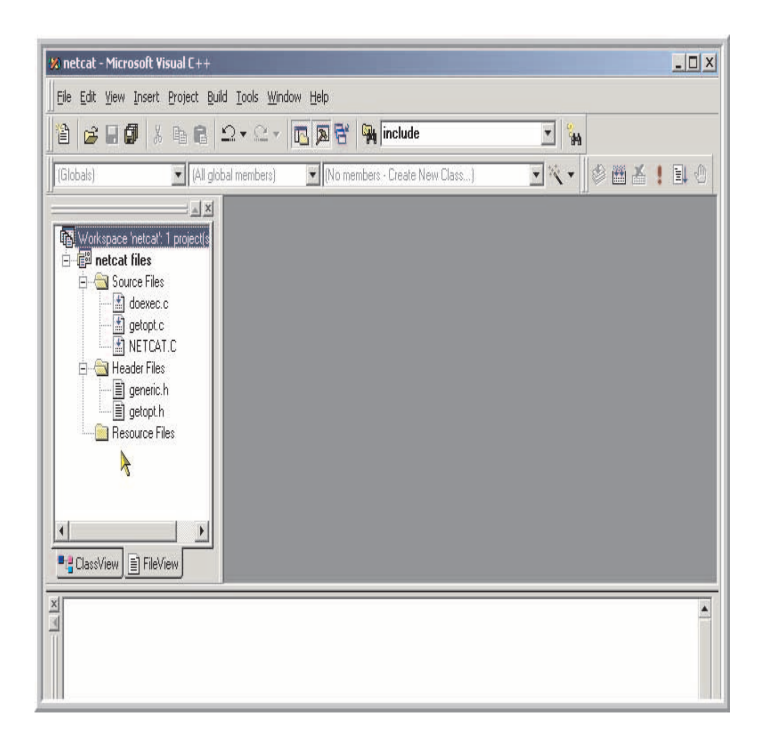
Los archivos con extensión h (*.h) son los llamados archivos de cabecera. Recuerda simplemente que es donde se

COMPILACION DEL NETCAT

nombran (definen) las funciones. Si, si, ya se que eso ahora no significa nada para ti, pero con que empiecen a sonarte estas palabras, ya me vale).

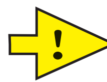
Los archivos con extensión c (*.c) es el código del programa a partir del cual se obtendrá en ejecutable.

No te cortes, pulsa sobre los simbolitos + y verás cómo han sido distribuidos los archivos :)



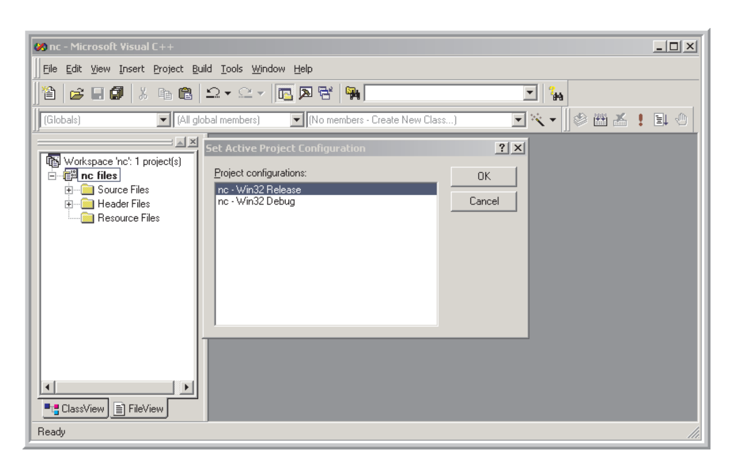
7.- Configurando el proyecto:

Menú Build --> Set Active configuration y en la ventana que aparecerá selecciona nc-Win32release y pulsa OK.



La opcion...

La opción Win32Debug sólo se utiliza en la fase de desarrollo de cualquier programa, por lo que por ahora, no nos interesa.

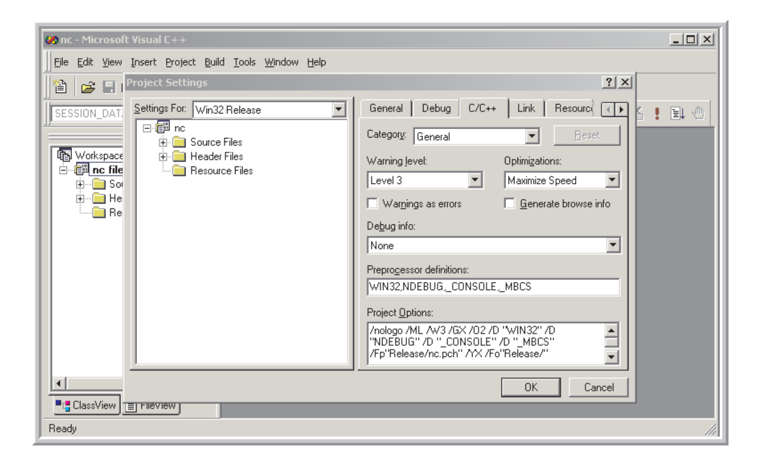


Ahora introduciremos las opciones de compilación que, normalmente, se encuentran en el archivo de nombre makefile. Abre la carpeta donde descomprimiste el netcat (c:\nc) y verás que uno de los archivos descomprimidos es el makefile (tal cual, sin extensión).
Este archivo sin extensión puedes abrirlo directamente con cualquier editor de texto e incluso con el bloc de notas, pues venga, lo abrimos y obtenemos esto:

```
cc=cl
link=link
cflags=/nologo /ML /W3 /GX /O2 /D "NDEBUG" /D "WIN32" /D "_CONSOLE" /D "TELNET" /D "GAPING_SECURITY_HOLE" /YX /FD /c
lflags=kernel32.lib user32.lib wsock32.lib winmm.lib /nologo /subsystem:console /incremental:yes /machine:I386 /out:nc.exe
all: nc.exe
getopt.obj: getopt.c
    $(cc) $(cflags) getopt.c
doexec.obj: doexec.c
    $(cc) $(cflags) doexec.c
netcat.obj: netcat.c
    $(cc) $(cflags) netcat.c
nc.exe: getopt.obj doexec.obj netcat.obj
    $(link) getopt.obj doexec.obj netcat.obj $(lflags)
```

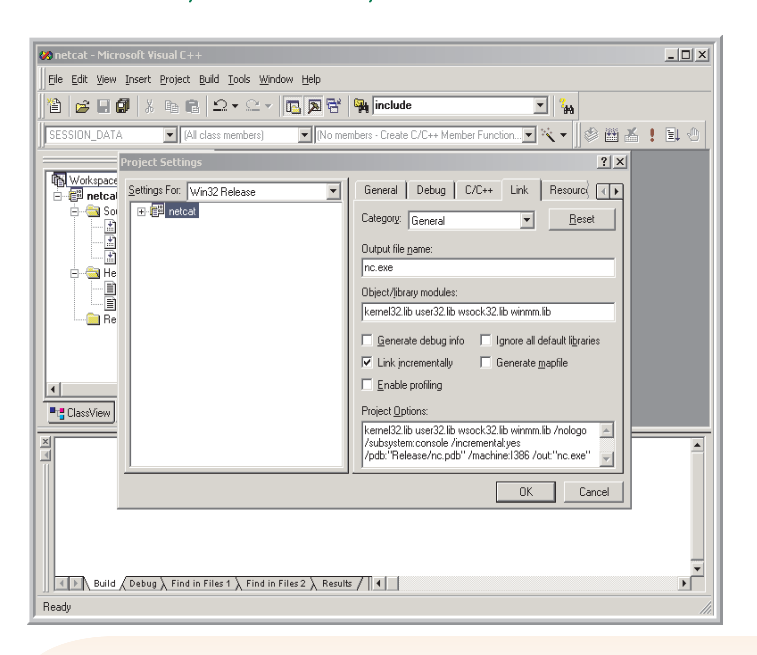
Ahora nos vamos al Menú Project --> Settings y en la ventana que aparecerá selecciona la pestaña C/C++

COMPILACION DEL NETCAT



Borramos todo lo que ponga en Project Options (abajo a la derecha) y ponemos lo que sale en el makefile después de cflags= (en azul), es decir: /nologo /ML /W3 /GX /O2 /D "NDEBUG" /D "WIN32" /D "_CONSOLE" /D "TELNET" /D "GAPING_SECURITY_HOLE" /YX /FD /c. Fíjate que cuando pegues este texto, la sección "C/C++" se autocompletará.

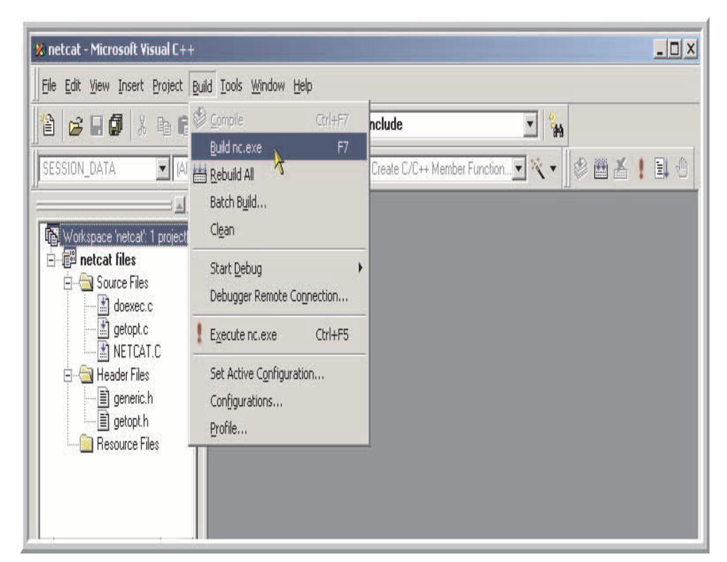
Ahora vamos a la pestaña Link, borramos todo lo que ponga en Project Options y ponemos lo que sale en el makefile después de lflags= (en verde), es decir: kernel32.lib user32.lib wsock32.lib winmm.lib /nologo /subsystem:console /incremental:yes /machine:I386 /out:nc.exe



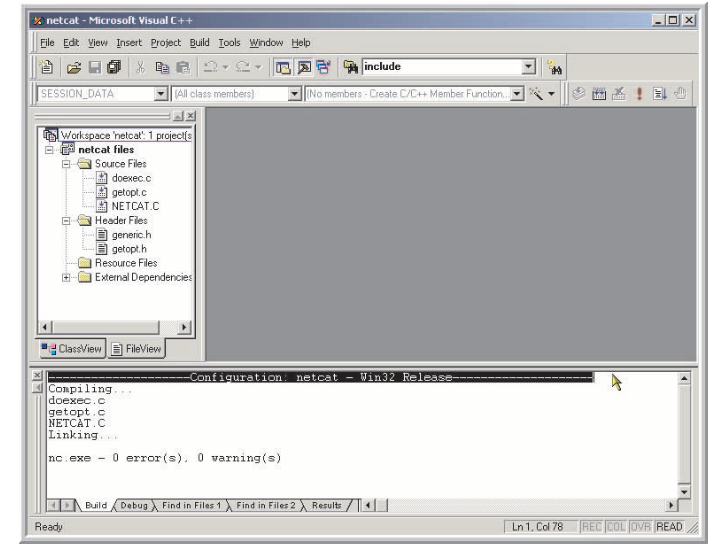
Finalmente pulsamos OK.

8.- Compilando... ...

Ya está todo preparado para compilar el código y obtener el ejecutable del netcat (nc.exe). Venga, vamos al Menú Build --> Build nc.exe

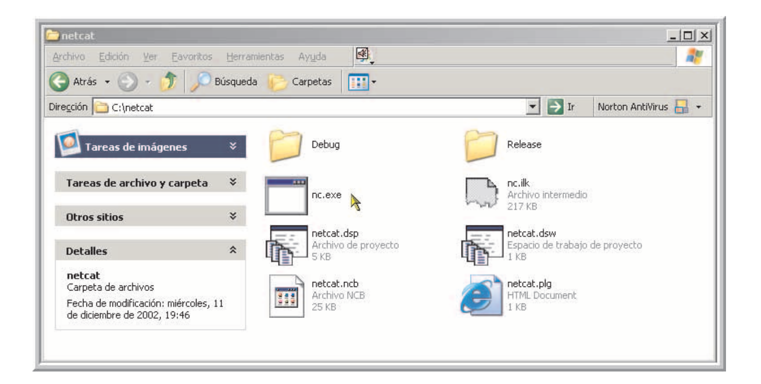


... y veremos como se inicia la compilación, puedes ver el proceso en la ventana blanca de abajo: **Configuration: netcat -Win32**



Ahora visita tu carpeta c:\netcat y encontrarás a tu flamente nc.exe ;)

COMPILACION DEL NETCAT



Ya está, ya has compilado tu propio netcat ;)

10.- Unas cuantas cositas...

Quizás te estés preguntando qué son todos esos archivos que han aparecido en la carpeta netcat. Bien, pues te explico un poquito (solo un poquito). Resumiendo y sin entrar en detalles, tu le has dado al compilador los archivos *.c y *.h (al principio del artículo, ¿recuerdas?) Bien, pues él los ha cogido y cuando le has dicho que compile el netcat (Build nc), a partir de ellos ha creado unos archivos *.obj (ficheros objeto) en la carpeta release (acuérdate que le dijimos que queríamos la opción de Win32release). A este proceso se le llama compilado y es un paso intermedio mediante el cual el compilador reúne los datos necesarios para el paso siguiente, para no entrar en tecnicismos y siendo muy poco escrupulosos (es decir, siendo verdaderamente bestias) podemos decir que convierte a "código máquina" las instrucciones que figuran en los archivos *.c y *.h.

En el paso siguiente, llamado linkado, el Visual C++ utiliza esos *.obj para acabar de obtener todos los elementos que permitirán finalmente crear nuestro netcat. No podemos detallarlo más porque realmente el tema es complejo y extenso... todo llegará.

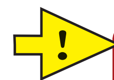
El archivos NETCAT.dsw es el espacio de trabajo (como la mesa donde trabaja un administrativo), el archivo NETCAT.dsp es el proyecto Netcat y los demás, digamos que aceleran la compilación ;p

La intención de este artículo era acercarte un poco al mundillo de los compiladores y hacer que pierdas el miedo a todo eso :)

11.- Otra forma de compilar ;p

Je, je, no te enfades ¿vale? Podrías haberte ahorrado todo esto abriendo una Ventana de Comandos, metiéndote en el directorio donde descomprimiste el código fuente del nc (c:\nc) e introduciendo la instrucción nmake y pulsando enter.

Se acabó, te habrá compilado el netcat y habrá creado el archivo nc.exe en esa misma carpeta. Pero ya nos conoces, no podíamos ponértelo tan fácil ;p



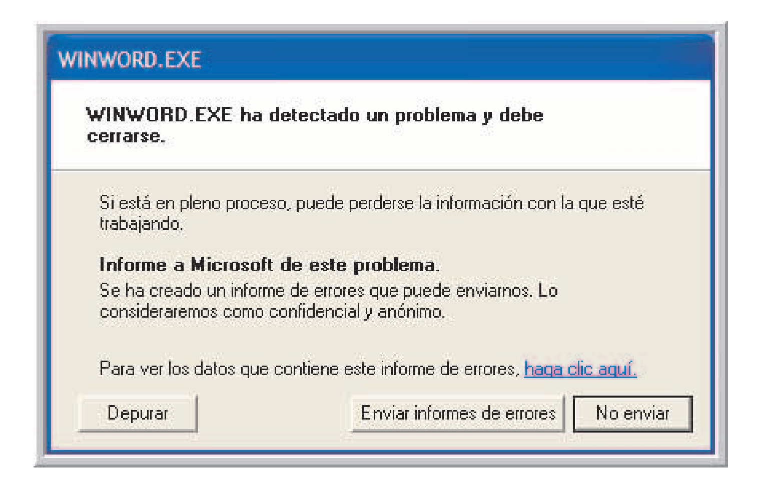
Para poder...

Para poder hacerlo así, tienes que tener el Visual C++ instalado y las variables de entorno registradas :)



BUGS, ERRORES Y OTRAS FORMAS DE JOD...

¿Quién no ha ejecutado un programa bajo Güindous y le ha aparecido algo como esto?



Y ha tenido que volver a empezar un trabajo de 15 páginas para el cole, la novia, el curro, una REVISSSSSSTA, etc. Por que para quien no lo sepa WINWORD.EXE es el famoso WORD. Y pensar que gracias a estos BUGS, unos se ganan la vida y el resto estamos P*T**D*S.

-¡Pero si WORD es de MICRO-PIIIIIII! ¡Debería ser compatible al 100% con WINDOWS!

Y lo es, sino, pregúntaselo a Hill Gates. Que va a decir el pobre ;).

¿Por qué se producen los errores en los programas?
¿Son tan malos los programadores?

Según la propietaria del MUNDO del PC (o casi), la mayor parte de los errores se producen por una mala utilización del SOFT por parte del usuario.
-Eso significa que un usuario ha usado mal la conversión de UNICODE a ASCII, reventando así un servidor con IIS instalado!!!

Según Micro... Sí. En honor a la verdad, de vez en cuando, reconocen que meten la pata, pero como el negocio es suyo, pues nada, a tragar mas BAZZZUURAAAA (dos velas negras !!!).

¿Por qué se producen los BUGS?

Para la gente que sepa algo de programación, los errores se producen por una mala planificación del proyecto (en el 90% de los casos esto es falso), este es demasiado grande ó complejo y es difícil de prever todas las situaciones posibles en donde el soft se ubicará.

Realmente si todo fuera bien y funcionase perfectamente, nadie cambiaría lo que tiene y el negocio se acabaría y ...

¿Hacen malos programas queriendo?

Un momento, que no he acabado. Nadie tira piedras sobre su propio tejado, pero la verdad es que hay ERRORES, BUGS, y demás pifias informáticas que huelen muy mal.

Ejemplo:
WINDOWS NT 4.0 vio la luz en 1996, estamos en 2003 y parte de sus errores han sido heredados por Windows 2000 y Windows XP. Una parte muy pequeña, pero suficiente para que nos divirtamos un poco :).

El verdadero origen de todo mal, suele venir, y valga la REBUZNANCIA, del origen del soft, el ...

-El programador claro!!!

Eres más rápido hablando que pensando, por eso no me extraña que tartamudees. El origen del soft es el lenguaje de programación y sus herramientas.

¿A que qué?

Visual Studio, Visual C++, Visual Basic y un largo etc.

¿A que qué? II

Léete el número IV con el OSITO (PC PASO A PASO 4)

Continuando por donde lo dejé, lo explicare mejor:

> El programador dice al ordenador que imprima un texto en pantalla.
>
> El ordenador lo hace.

Todo correcto hasta que alguien descubre que la función de imprimir en pantalla tiene un error que hace que se bloquee el equipo.

El programador se ha equivocado!!!

Sí, por confiar en que la función imprimir en pantalla es buena, tiene que serlo, ha de serlo, le ha costado 2.600€ , y si es tan caro y de M*CR*S*FT, ha de ser muy bueno.

También los primeros Pentium no sabían dividir, pero como son de INTEL da igual.

El problema tiene difícil solución, porque el dueño de las herramientas de desarrollo, no puede saber que narices hace internamente la función imprimir en pantalla, ni las tropecientasmil y pico funciones más que tiene a su disposición, porque M*CR*S*FT no le facilita el CODIGO-FUENTE (listado de las operaciones básicas que realiza cada función) no quiere que se las copien - imiten -calquen- reproduzcan - dupliquen - fusilen, etc. Sólo le queda confiar en el buen hacer de Microsoft, en que los políticos digan la verdad y que todos seamos muy felíces.

PD. Dime con que compilas y te daré las gracias.



Firma utilizada por Pringle en el foro de HackXCrack. Te la tomamos "prestada", que es muy buena ;)

SERVIDOR DE HXC
MODO DE EMPLEO

- Hack x Crack ha habilitado un servidor para que puedas realizar las prácticas de hacking.

- Actualmente tiene el BUG del Code / Decode y lo dejaremos así por un tiempo (bastante tiempo ;) Nuestra intención es ir habilitando servidores a medida que os enseñemos distintos tipos de Hack, pero por el momento con un Servidor tendremos que ir tirando (la economía no da para mas).

- En el Servidor corre un Windows 2000 Advanced Server con el IIS de Servidor Web y está en la IP 80.36.230.235.

- El Servidor tiene tres unidades:
* La unidad c: --> Con 2GB
* La unidad d: --> Con 35GB y Raíz del Sistema
* La unidad e: --> CD-ROM

Nota: Raíz del Servidor, significa que el Windows Advanced Server está instalado en esa unidad (la unidad d:) y concretamente en el directorio por defecto \winnt\ Por lo tanto, la raíz del sistema está en d:\winnt\

- El IIS, Internet Information Server, es el Servidor de páginas Web y tiene su raíz en d:\inetpub (el directorio por defecto)

Nota: Para quien nunca ha tenido instalado el IIS, le será extraño tanto el nombre de esta carpeta (d:\inetpub) cómo su contenido. Pero bueno, un día de estos os enseñaremos a instalar vuestro propio Servidor Web y detallaremos su funcionamiento.

De momento, lo único que hay que saber es que cuando TÚ pongas nuestra IP (la IP de nuestro servidor) en tu navegador, lo que estás haciendo realmente es ir al directorio d:\Inetpub\wwwroot\ y leer un archivo llamado default.htm.

Nota: Como curiosidad, te diremos que APACHE es otro Servidor de páginas Web (seguro que has oído hablar de él). Si tuviésemos instalado el apache, cuando pusieses nuestra IP en TU navegador, accederías a un directorio raíz del Apache (donde se hubiese instalado) e intentarías leer una página llamada index.html

Explicamos esto porque la mayoría, seguro que piensa en un Servidor Web como en algo extraño que no saben ni donde está ni como se accede. Bueno, pues ya sabes dónde se encuentran la mayoría de IIS (en \Inetpub\) y cuál es la página por defecto (\Inetpub\wwwroot\default.htm). Y ahora, piensa un poco... ... ¿Cuál es uno de los objetivos de un hacker que quiere decirle al mundo que ha hackeado una Web? Pues está claro, el objetivo es cambiar (o sustituir) el archivo default.html por uno propio donde diga "hola, soy DIOS y he hackeado esta Web" (eso si es un lamer ;)

A partir de ese momento, cualquiera que acceda a ese servidor, verá el default.htm modificado para vergüenza del "site" hacheado. Esto es muy genérico pero os dará una idea de cómo funciona esto de hackear Webs ;)

- Cuando accedas a nuestro servidor mediante el CODE / DECODE BUG, crea un directorio con tu nombre (el que mas te guste, no nos des tu DNI) en la unidad d: a ser

posible (que tiene mas espacio libre) y a partir de ahora utiliza ese directorio para hacer tus prácticas. Ya sabes, subirnos programitas y practicar con ellos :)

Puedes crearte tu directorio donde quieras, no es necesario que sea en d:\mellamojuan. Tienes total libertad!!! Una idea es crearlo, por ejemplo, en d:\winnt\system32\default\mellamojuan (ya irás aprendiendo que cuanto mas oculto mejor :)

Es posiblemente la primera vez que tienes la oportunidad de investigar en un servidor como este sin cometer un delito (nosotros te dejamos y por lo tanto nadie te perseguirá). Aprovecha la oportunidad!!! e investiga mientras dure esta iniciativa (que esperamos dure largos años)

- En este momento tenemos mas de 600 carpetas de peña que, como tu, está practicando. Así que haznos caso y crea tu propia carpeta donde trabajar.



MUY IMPORTANTE...

MUY IMPORTANTE!!!!! Por favor, no borres archivos del Servidor si no sabes exactamente lo que estás haciendo ni borres las carpetas de los demás usuarios. Si haces eso, lo único que consigues es que tengamos que reparar el sistema servidor y, mientras tanto, ni tu ni nadie puede disfrutar de él :(Es una tontería intentar "romper" el Servidor, lo hemos puesto para que disfrute todo el mundo sin correr riesgos, para que todo el mundo pueda crearse su carpeta y practicar nuestros ejercicios. En el Servidor no hay ni Warez, ni Programas, ni claves, ni nada de nada que "robar", es un servidor limpio para TI, por lo tanto cuídalo un poquito y montaremos muchos más :)

NETBIOS: ESTUDIO Y PENETRACION DE SISTEMAS

PARTE I: TOMA DE CONTACTO E INTRUSIÓN

1.- ¿QUÉ ES NETBIOS?

¿Por dónde empiezo? Tengo 10 páginas para explicar qué es, cómo funciona y algún método de "penetración"... buffff, es una lastima que esta revista no tenga más páginas, porque hay mucho que explicar, bueno, empecemos...

Hacemos un rápido viaje en el tiempo y nos vamos a 1984. IBM diseña un sistema "application programming interface" (API) para conectar en red sus computadoras y lo llamó Network Basic Input/Output System (NetBIOS). Esta API era un sencillisimo sistema para permitir a un pc conectarse con otro para poder intercambiar datos. Pero en aquella época, hacer que una máquina "hable" con otra totalmente distinta era difícil (los ordenadores no eran muy stándares que digamos), por lo que en 1995, IBM "inventó" un "protocolo de transporte", es decir, unas "normas" que, si todos los PCs cumplían, permitía que unos hablasen con otros. Este protocolo unido a la API dio lugar a lo que se llamó NetBIOS Extended User Interface (NetBEUI). Venga, no te duermas, que la clase de historia ya se acaba ;)

Hasta ahora hemos visto el "mundillo" de las Ips en los números anteriores, bien, pues el NetBEUI funciona de forma parecida pero en lugar de utilizar Ips utiliza NOMBRES.

Imagina una habitación en la más absoluta oscuridad con una mesa en el centro y 10 sillas alrededor con una persona sentada en cada silla, imagina que tienen que empezar a debatir sobre algún tema importante pero los interlocutores no se conocen y no pueden verse... ummm... hay un problema, cuando alguien hable no serás capaz de "identificarlo", y si dos personas tienen una voz parecida, ya ni te cuento. Como tu eres el moderador y eres muy listo, les dices que al inicio de cada intervención deben pronunciar su nombre, de esta forma todos sabemos quién está hablando en cada momento. Muy bien, pues eso es lo que hace esa cosa que hemos llamado NetBEUI, establecer unas normas de conducta.

Imagina ahora que se añade una silla más y una persona entra en la sala (Inicio de sesión). Según el protocolo (el NetBEUI), esa persona debe presentarse al resto de miembros diciendo su nombre y tomar asiento, pero no todo es tan sencillo, imagina que el nuevo "tertuliano" se llama Juan y ya había otra persona llamada Juan sentada en la mesa. CONFLICTO!!! Recuerda que la habitación está a oscuras, si hay dos personas con el mismo nombre no podremos distinguirlas correctamente, por lo tanto se le deniega el acceso (inicio de sesión) y se le "invita" (obliga) a cambiar de nombre o adios muy buenas.

Todo eso ocurre cuando un ordenador quiere entrar a formar parte del resto de la "red" (resto de tertulianos) en un sistema NetBEUI, el PC que quiere meterse en la red debe dar un nombre y ese nombre no puede ser repetido en una misma red.

Este protocolo (NetBEUI) empezó ser muy utilizado por las aplicaciones de red y por

aquella reliquia llamada Windows para Grupos (alguien la recuerda? ;)). En aquella época el NetBEUI competía con el IPX de Novell, otro protocolo del que no hablaremos porque este mes "no toca", y como siempre ocurre, se crearon las implementaciones de NetBEUI para IPX, es decir, que las máquinas basadas en NetBEUI finalmente podían "relacionarse" con las redes IPX. Y a todo esto, paralelamente, nos encontramos con los protocolos elejidos para Internet: TCP/IP. Pues lo mismo, en poco tiempo salieron implementaciones del NetBEUI para que pudiese "hablar" con redes basadas en TCP/IP.

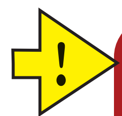
- Muy interesante, pero por qué me explicas todo eso, yo lo que quiero es estudiar esos procesos de "penetración" que...

NO!!!, lo primero es lo primero, es necesaria una pequeña "toma de contacto" antes de lanzarte a la conquista de Internet, recuerda que solo el conocimiento te hace libre ;P

Sigamos... ah, si... ahora tenemos un problema!!! El TCP/IP funciona a base de Ips (ya lo explicamos en anteriores números) y el NetBEUI funciona a base de nombres (si, si, nombres tan sencillos como Carlos, PC5 o PCPRINCIPAL), así que en 1987 (si no me falla la memoria) el IETF (Internet Engineering Task Force) publicó los RFC 1001 y 1002 (RFC son documentos donde se detalla prácticamente todo lo relacionado con la tecnología de la que se sirve Internet: protocolos, recomendaciones, comunicaciones...). Muy bien, pues esos documentos son en los que se basan actualmente tanto Microsoft con su "Compartir Impresoras y Archivos para redes Microsoft) como Linux con su SAMBA, tanto uno como otro son la evolución del NetBEUI, llamada posteriormente NETBIOS SOBRE TCP/IP y se utilizan para montar mesas (sesiones) con tertulianos (PCs) deseosos de compartir información ;) repartidos por cualquier rincón de Internet.

Venga, que ya acabo!!! El NETBIOS SOBRE TCP/IP es conocido como NBT (como le gusta a los "genios" machacarnos a los pobres mortales con siglas y mas siglas es increible) y se basa en tres servicios: Un servicio de nombres y dos servivios de comunicaciones (datagramas y sesiones). El primero, el servicio de nombres, resuelve (implementa) la relación NOMBRE-IP, es decir, gestiona la relación entre un NOMBRE y su IP. Los otros dos se utilizan para gestionar la transmisión de datos.

- ¿Ya has acabado?
Bueno, porque el director me ha dicho que debo ser breve, que si no, escribo 50 folios sobre todo esto... venga, si, ya he terminado :)

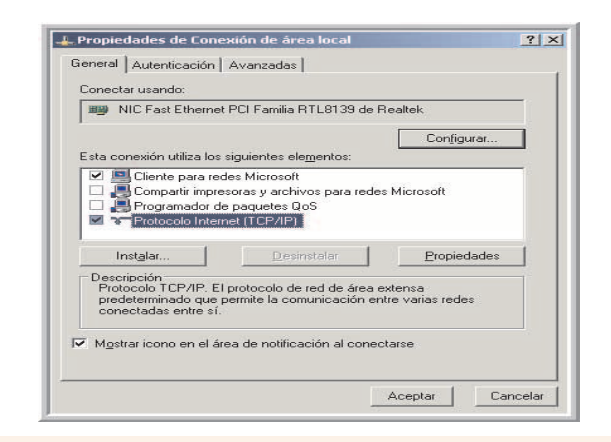


Resumen...

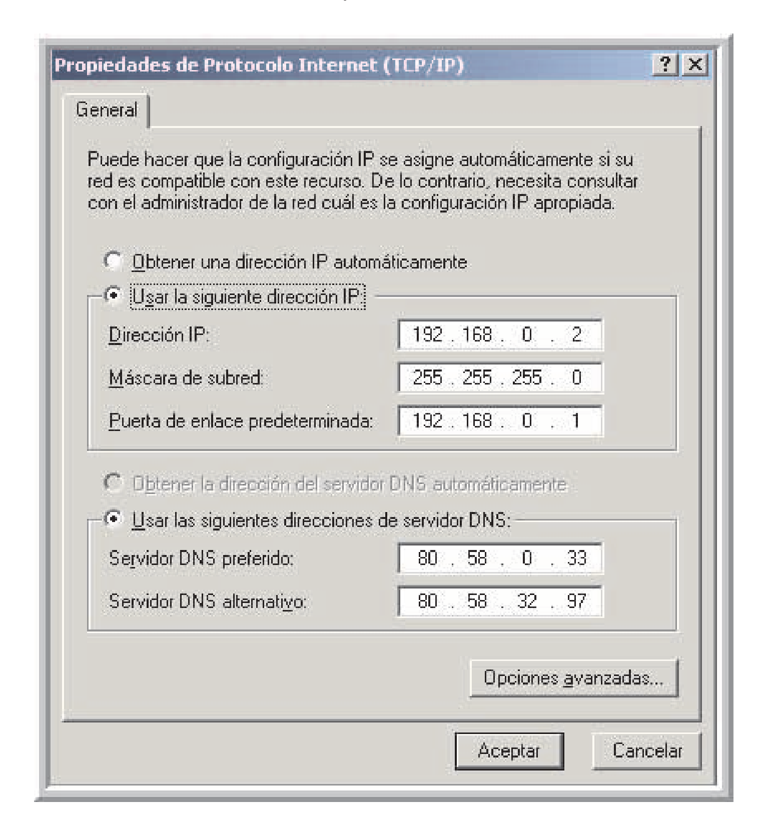
Resumen/Detalles importantes: El NETBIOS es un protocolo/servicio que te permite compartir recursos entre ordenadores (como por ejemplo tus discos duros). Este servicio está a la escucha en los puertos 137, 138 y 139 (esto de los puertos ya sabes como funciona de otros números)

2.- El NETBIOS en nuestro Windows.

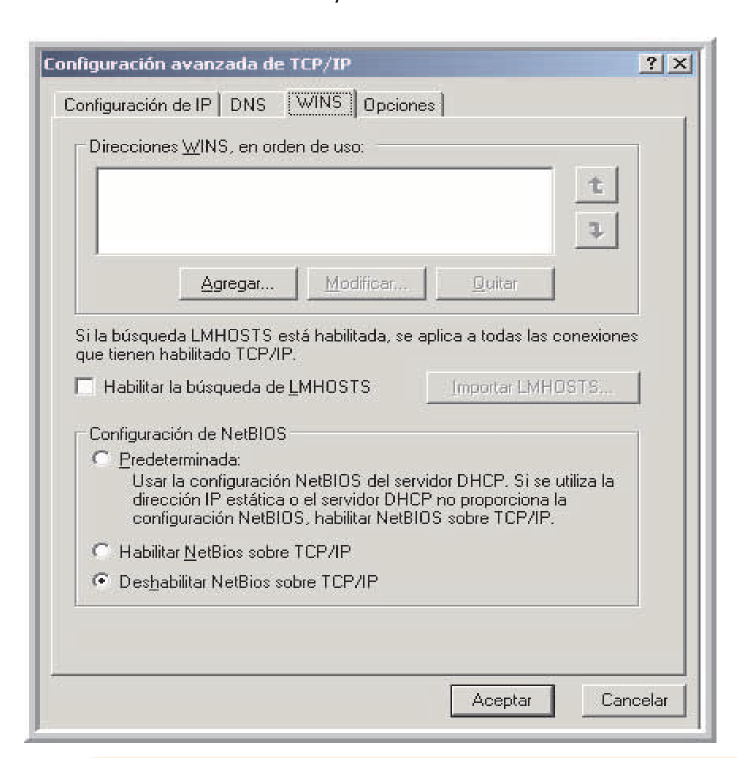
Ahora, para ver "de cerca" eso del NETBIOS, nos vamos a nuestras conexiones de red,



nos metemos en las Propiedades del Protocolo Internet TCP/IP



nos metemos en las Propiedades del Protocolo Internet TCP/IP



podrás ver que puedes gestionar si deseas Netbios (o no) en tu Windows XP.

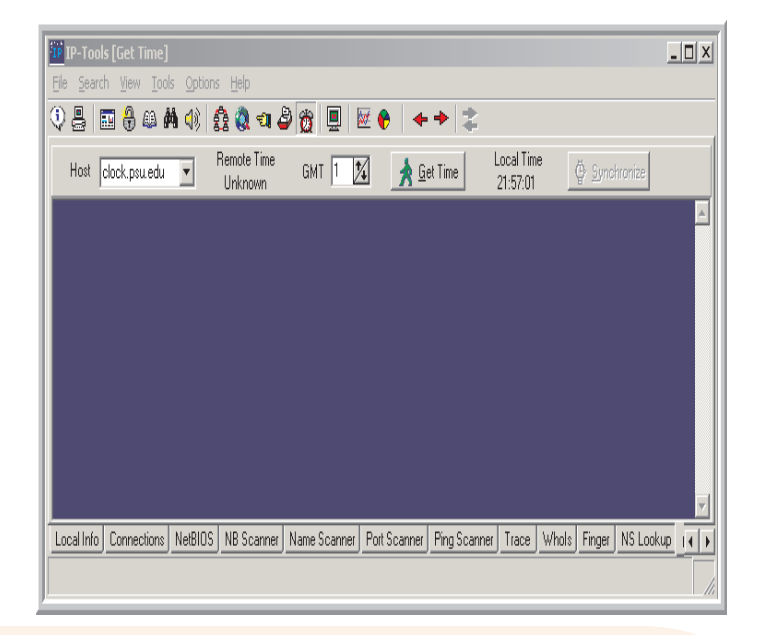


El mes que viene explicaremos la forma de configurar el sistema para dejar proteger un poco yu sistema de los ataques por NETBIOS y lo explicaremos para cada sistema Windows. Las imágenes ateriores son de Windows XP.

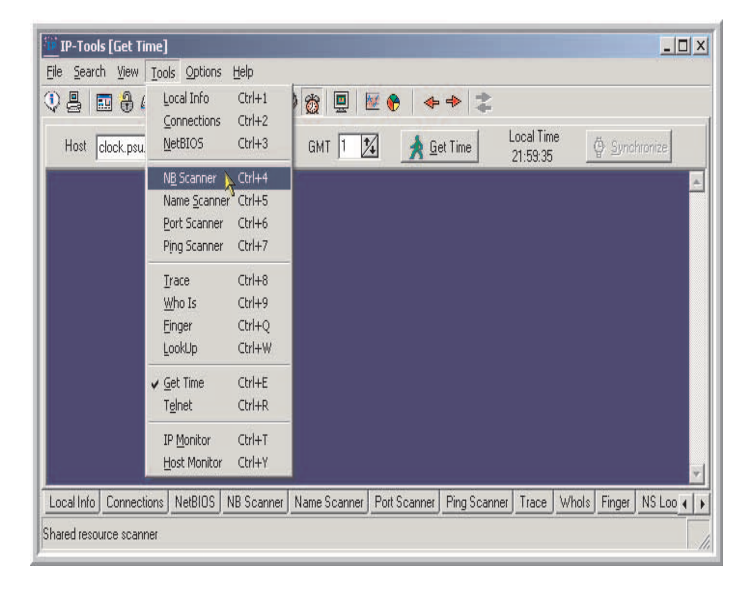
3.- Escaneando máquinas con NETBIOS :)

Bueno, vamos a empezar a divertirnos :)

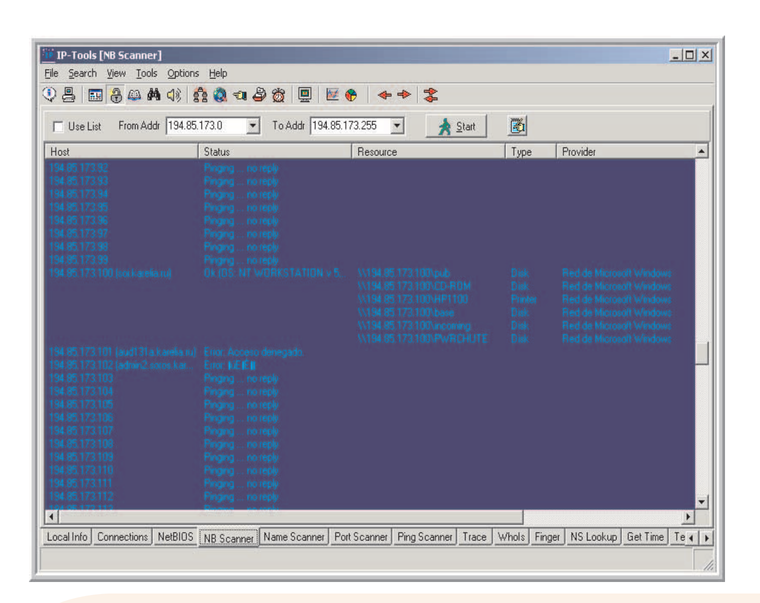
Lo primero que necesitamos es un escaneador de IPs que apunte a los puertos 137, 138 y 139, los puertos que utiliza NETBIOS. Como no tenemos ninguna víctima en mente, escanearemos Internet buscando máquinas con esos puertos abiertos mediante el software IP-TOOLS (lo encontrarás en http://www.ks-soft.net o en nuestra Web www.hackxcrack.com). Una vez descargado, lo instalamos, ejecutamos y nos encontraremos con esto:



Nos vamos al Menu Tools --> NB Scanner (si, si, eso que vimos en la clase de historia ;)

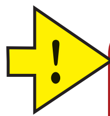


Ahora introducimos un rango de Ips. Arriba, donde pone From Addr, pondremos la IP inicial del rango que queremos escanear y en To Addr la IP final. Un día de estos explicaremos algunas "cositas interesantes" sobre la selección de rangos para escanear, pero por ahora nos conformaremos con introducir un rango al azar, por ejemplo del 194.85.173.0 al 194.85.173.255 y pulsaremos START (el hombrecito verde). Veremos como el programa empieza a trabajar y no tardará mucho en encontrar una IP-VÍCTIMA, en este caso la 194.85.173.100 :)



Fíjate bien en la cantidad de información que nos da el programa de la IP 194.85.173.100:

- Host: aud131a.karelia.ru --> El nombre del dominio, que nada tiene que ver con el nombre de NETBIOS. En el número 1 de PC PASO A PASO (Los cuadernos de Hack x Crack) encontrarás qué es eso de los nombres de dominio, lo tienes GRATIS para descargar en www.hackxcrack.com.
- Status: OS NT WORKSTATION 5 (el sistema operativo de la víctima)
- Resource: los elementos "compartidos"
- Type: tipo de elemento (si es una impresora, un disco duro… …)
- Etc.



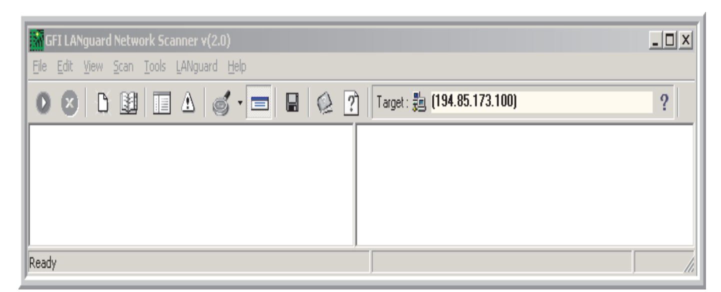
Puedes utilizar...

Puedes utilizar cualquier scanner, simplemente tienes que configurarlo para buscar los puertos 137, 138 y 139 abiertos. Nosotros hemos utilizado el IP-TOOLS porque es una herramienta muy interesante que creemos deberías probar… je, je… es una especie de todo en uno ;)

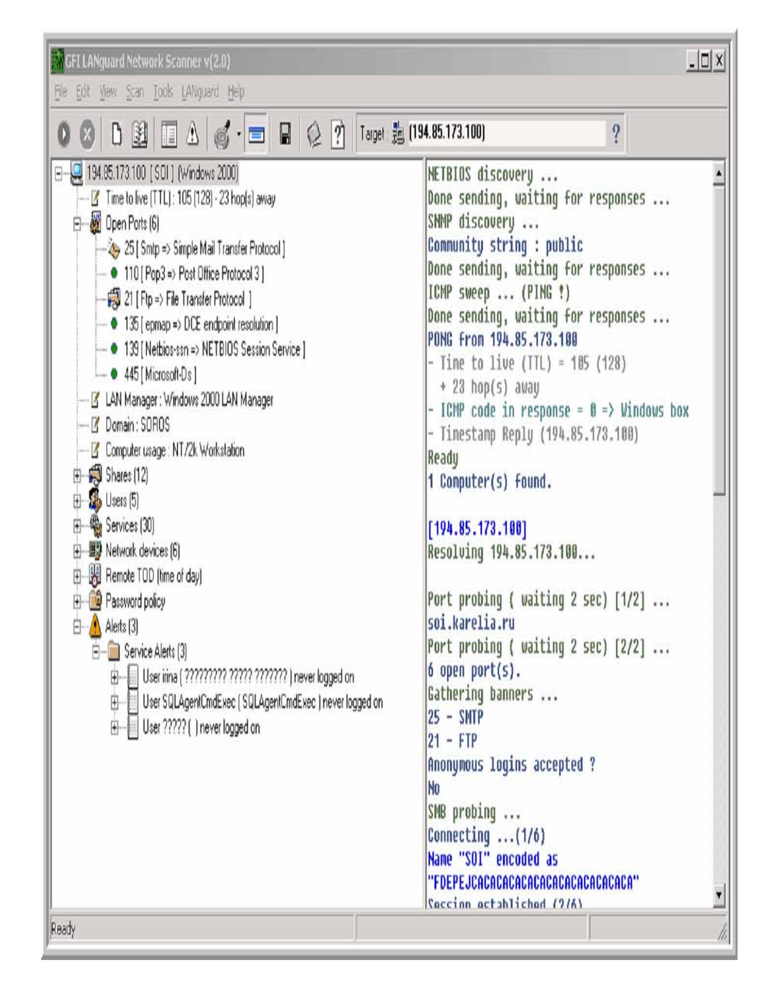
4.-Estudiando a la víctima:

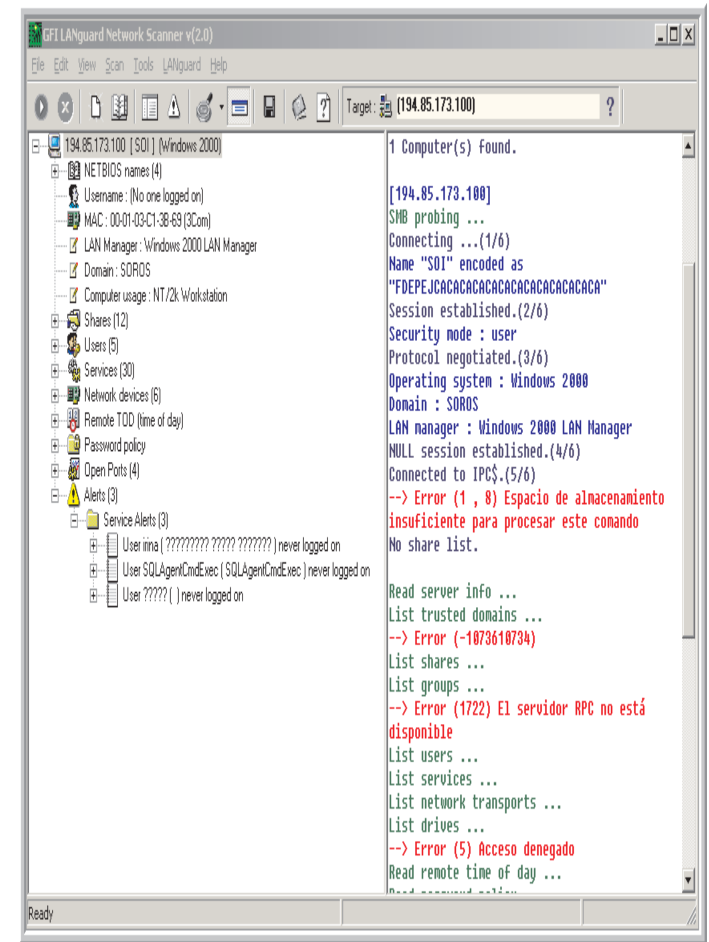
Una vez encontrada una posible víctima, vamos a intentar presentarnos y para eso necesitaremos el LANGUARD NETWORK SCANNER, programa que encontrarás en nuestra Web (www.hackxcrack.com)

Pues venga, lo descargamos, ejecutamos y nos encontraremos frente a esto



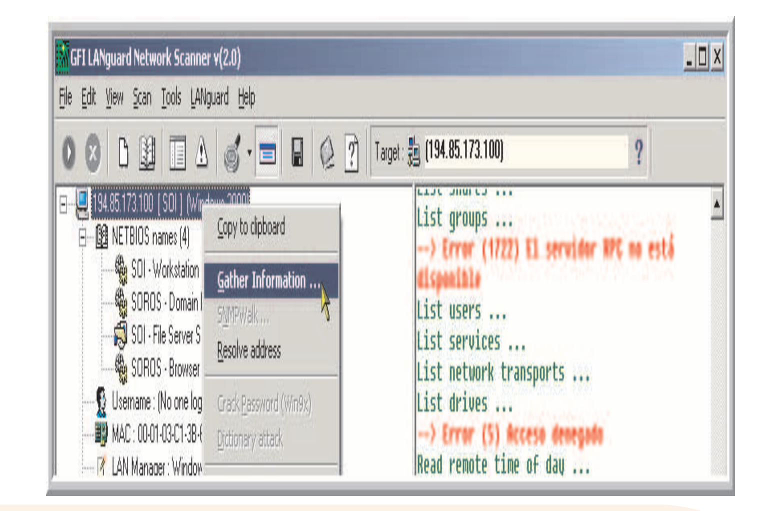
Para introducir la IP-VICTIMA nos vamos al Menu File --> New Scan, seleccionamos Scan One Computer y la introducimos.





Pulsamos FINISH y volveremos a la ventana principal del programa, pues venga, empieza la fiesta, pulsa el botón de PLAY (está arriba a la izquierda). Obtendremos un montón de datos, sería realmente interesante explicar cada uno de ellos pero no hay más espacio, quizás en el próximo número, me interesa más que una vez dentro practiques los comandos que te detallamos al final de este artículo ;)

Ahora, arriba a la izquierda, pon el mouse sobre la ip, pulsa con el botón derecho del Mouse y en el Menu contextual selecciona Gather Information..., esto nos ofrecerá más información de la "victima", por ejemplo el usuario, discos duros compartidos, etc.

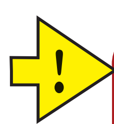


Ahora, si la víctima fuese un Windows 9X en lugar de un Windows 2000 y pusiesemos el mouse sobre la IP y abriesemos el menu contaxtual (botón derecho del mouse), un poco más debajo de la opción Gather Information estaría "iluminada" la opción Crack Password, con lo que obtendríamos directamente el password de la víctima, así de fácil. :)

Como esto en un Windows 2000, pues no podemos hacer eso, por lo que tendríamos que utilizar un diccionario de claves (está en el mismo menu) o utilizar una técnica de "null connect" que no explicaremos hoy. Después del uno va el dos, y estamos en el primer artículo de NETBIOS, antes de enfrentarte a un Windows 2000 tendrás que "trastear" un poco con máquinas Windows 9X y con los comandos que hay al final de este artículo :)

5.- Entrando en la víctima:

Si estuviesemos ante un Windows 9X ya tendríamos la clave y procederíamos a la entrada al sistema y eso es lo que vamos a explicar ahora, pero antes te "relato" cómo averigua el LANGUARD NETWORK SCANNER la tan apreciada clave.



Sobre cómo...

Sobre cómo el LANGUARD NETWORK SCANNER averigua la clave en un Windows9X: Pues es muy sencillo, de verdad, je, je… Imagina que tienes un hermano pequeño (como de 10 años) un poco tonto, le dices que piense en una palabra y le aseguras que TU averiguarás esa palabra.

Tu hermano se rie de ti y piensa en una palabra, por ejemplo ABCK

Tu, que eres muy listo, en lugar de empezar a soltar posibles palabras (diccionario de claves) le preguntas a tu hermano si la primera letra es una A, a lo que responde que si (ya tenemos la primera letra). Le preguntas si la segunda letra es una A y te dice que no, le preguntas si la segunda letra es una B y te dice que si (ya tenemos AB). Ahora haces lo mismo para la tercera (sigues el abecedario) y cuando le preguntas si es una C te dice que si (ya tenemos ABC). De nuevo le preguntas por la cuarta letra recorriendo el abecedario y cuando llegues a la K te responderá afirmativamente. Se acabó, ya tienes la palabra (clave): ABCK. Tu hermano, sorprendidisimo te mirará y adorará por el resto de tus días, je, je :)

Hemos dicho que tu hermano tenía que ser un poco tonto para no darse cuenta de que le estás sacando la palabra de una forma tan tonta, pues en este caso, tu hermano pequeño es Microsoft con su Windows 9X ;), así es como el LANGUARD averigua la clave de la víctima: preguntando letra a letra.

¿ASUSTADO?!!! ¿Piensas ahora en las horas que has pasado INDEFENSO conectado con tu Windows 9X? Bueno, dale las gracias a Bill Gates ;p. A ver si en el próximo número te enseñamos cómo configurar tu equipo para defenderte de esto, que este mes no hay espacio.

- Entrando a lo lamer y sin aprender nada: Una vez crackeado el pasword con el LANGUARD, simplemente haz un doble click sobre la IP y tendrás a tu disposición las unidades disponibles, así de simple :)

- Entrando y aprendiendo, como debe ser:

 * Abrimos una Ventana de Comandos
 * Introducimos el comando net use x:\\xxx.xxx.xxx.xxx\c$ /user:yyyyyy (y pulsamos enter)



Explicación...

Explicación de la linea use x:\\xxx.xxx.xxx.xxx\c$ /user:yyyyyy

- net use: Te enseña información sobre las conexiones o te conecta/desconecta de un recurso compartido.
- x: es el nombre que le asignaremos en nuestro equipo al recurso que intentas acceder. Imagina que intentas acceder al un recurso compartipo de la víctima llamado disco4, pues en tu equipo aparecerá un nuevo "recurso" llamado x (puedes poner el nombre que quieras)
- xxx.xxx.xxx.xxx: la IP de la víctima
- c$: sería la/el unidad/recurso compartida/o por la víctima.
- /user:yyyyyy --> El usuario

Un ejemplo de intrusión una vez crackeado el password sería:

Net use victima1:\\xxx.xxx.xxx.xxx\c$ /user:manolito

* Ahora nos preguntarían el password, pues nada, lo introducimos.

* Finalmente, te vas a MI PC y te encontrarás con un nuevo "disco duro" (recurso) llamado victima1 ;p

* Se acabó, entra en esa nueva unidad y utilizala como si fuese parte de tu PC ;)

6.- IDEAS/ADVERTENCIAS/NO SEAS MALO:

Puedes imaginarte la de cosas malas que puedes hacer, por ejemplo subir unos cuantos programitas y un win.ini modificado que haga referencia a unos cuantos programas para que sean ejecutados al en cada inicio del sistema y ya seguiremos otro día con esto, que estamos preparando un artículo al respecto :)

ASESINATOS COMETIDOS POR LA SSS-LSI

SOMOS EL PAIS MAS AVANZADO EN REPRESION INTERNAUTA

http://www.rolunlimited.tk
http://atlantida.archaeotour.com
http://www.villaricos.net
http://www.tolmo.com
http://www.tebusco.net
http://lomasretro.cjb.net
http://pauso.net
http://www.sabater.info
http://pagina.de/belcar
http://www.flyerbike.com
http://www.ciutatdemallorca.com
http://club.telepolis.com/txelienlinea/index.htm
http://www.bamdesigns.net
http://www.ias.as
http://www.leri-jardineria.com
http://www.farogroup.org
http://www.c-veca.com
http://www.anadef.com
http://www.hydrochip.com
http://www.marcianos.net
http://www.dudaelectronica.com
http://aered.net
http://www.todacantabria.com
http://csounds.com/jmc
http://garaje.ya.com/cchoni
http://www.glarester.com
http://www.kikolo.com
http://www.rockabillyrules.com
http://www.e-mataro.com
http://usuarios.lycos.es/malgusto
http://aesirmovil.iespana.es/aesirmovil
http://www.starcraft-esp.net
http://www.microswin.com
http://www.defzsounds.com
http://www.planetasim.es.vg
http://www.sexocurioso.com
http://www.losdemarras.rockk.net
http://www.geocities.com/riadepunta/index.html
http://www.hacklicante.com
http://es.geocities.com/bailen2008
http://www.taller3es.com
http://es.geocities.com/quioscovirtual
http://es.geocities.com/mispueblos
http://usuarios.lycos.es/casaforguar
http://www.fonsinieto.com
http://www.musicon-pro.com
http://www.puntaumbriadigital.com
http://www.surrealworks.com
http://www.artepop.com
http://www.buenrollito.com
http://www.artelinkado.com
http://www.canariaschat.com
http://go.to/bombprof
http://www.govannom.org
http://80.33.67.186/casulleras/ralliweb/index.htm
http://www.loswebs.cjb.net
http://arcoiris.tk
http://www.terra.es/personal2/gjvivac
http://www.sibuscas.com
http://www.marcianos.net
http://www.witep.com
http://www.gratisprogramas.net
http://www.dancefm.org
http://www.naymenos.com
http://www.glarester.com
http://www.areparar.com
http://www.ciutad.com
http://www.aconstruir.net
http://www.elfresno.com
http://www.iespana.es/tommy2ki
http://www.telecable.es/personales/frja1
http://www.balonmanoplaya.com
http://www.portaldehistoria.com
http://www.geocities.com/huelvacity
http://www.geocities.com/plazadecastilla
http://www.aquamp3.tk
http://www.winsms.org
http://www.bdftech.com
http://kung-foo.dhs.org
http://www.iespana.es/simples
http://www.recicla.com
http://www.finexs.com

UNA VERGUENZA EUROPEA

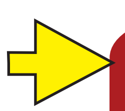
http://es.geocities.com/quioscovirtual
http://es.geocities.com/mispueblos
http://usuarios.lycos.es/casaforguar
http://www.fonsinieto.com
http://www.musicon-pro.com
http://www.puntaumbriadigital.com
http://www.kalitro.tk
http://www.lenguaje-c.es.vg
http://eureka.ya.com/biotec
http://usuarios.iponet.es/acosta
http://www.elprofe.info
http://www.dragonroms.com
http://usuarios.lycos.es/jovesaspe
http://www.defesta.com
http://www.simcitydeluxe.cjb.net
http://www.electric-bike.org
http://www.geocities.com/seleccionweb
http://www.geocities.com/callelimoneros
http://www.pulsatillarubra.com
http://www.lanzadera.com/automatismos
http://club.telepolis.com/rockabilly
http://personal.telefonica.terra.es/web/rockerparadise
http://www.televenta.org
http://www.televenta.info
http://www.correoelectronico.com
http://www.elchecomercios.com
http://www.mercaelche.com
http://www.emule-es.tk
http://www.karateelche.com
http://kemih.host.sk
http://www.elpelao.com
http://euitio.trisquelmedia.net
http://www.llorca.biz
http://www.almorox.net
http://ajedrezmania.com
http://es.geocities.com/crevillentwebring
http://es.geocities.com/mentsubita
http://pagina.de/santodomingodemoya
http://www.youthing.es
http://www.granollers.com
http://www.madridigital.net
http://divxtotal.dnsq.org
http://www.serveisabadell.com
http://www.lotano.com
http://www.e-mision.net/crazyhouse
http://www.focus-sl.com
http://www.tres-cantos.com
http://www.darkgnu.host.sk
http://www.russadir.com
http://www.seleccionnatural.com
http://www.muebles-abanico.com
http://catmoddingcase.port5.com
http://www.surestorm.com
http://www.cachoonda.com
http://zekson.net
http://www.principiantes.org
http://www.freestylebcn.tk
http://www.odiseaweb.com
http://www.elisoft.net
http://egiptologia.archaeotour.com
http://www.siero.com
http://www.iespana.es/clandeluxe
http://hosting.msnconfederacion.com/Sin_Clan
http://membres.lycos.fr/bernatpage
http://www.iespana.es/clanska
http://www.paisoscatalans.org/Canalunitat
http://www.geocities.com/revistamacondo
http://www.joyernet.com
http://fly.to/clubdefansdelgranhermano
http://icemanweb.iespana.es/icemanweb
http://www.z3r0.org
http://www.patapalo.net
http://www.datisa.net
http://www.uzart.org
http://moneo.yo.lv
http://www.valclip.com
http://www.lineaxxx.com
http://www.lainmobiliaria.org
http://www.magicogonzalez.com
http://www.fadlan.com
http://www.noctropolis.org
http://www.euskalnet.net/amesperuza
http://gente.chueca.com/kejeta
http://www.sabadellwireless.net

Y MUCHAS MÁS, PERO NO PODEMOS PONERLAS TODAS :(QUE LOS DIOSES NOS PROTEJAN AL RESTO.

LISTADO DE ORDENES PARA NETBIOS

A continuación colocaré un listado de todos los comandos NET muy bien detallados y con ejemplos para que sean más fáciles de entender.

Es recomendable que la mayoría de estos comandos sean bien aprendidos ya que son necesarios para usar correctamente el NetBios y poder manejarse dentro de otros sistemas.



Varios de los ...

Varios de los comandos de NET poseen algunas propiedades en común como:

- Se puede ver una lista de todos los comandos disponibles si escribe net/?
- Pueden obtener ayuda sobre la sintaxis en la línea de comandos para un comando net si escribe net help [comando]. Por ejemplo, si desea ayuda sobre el comando net accounts, escriba net help accounts.
- Todos los comandos net aceptan las opciones /yes y /no (se pueden abreviar como '/y' y '/n').

Lista de comandos: (Extraído de TImat)

'Net Accounts'

Actualiza la base de datos de cuentas de usuario y modifica los requisitos de contraseña e inicio de sesión para todas las cuentas.

net accounts [/forcelogoff:{minutos | no}] [/minpwlen:longitud] [/maxpwage:{días | unlimited}] [/minpwage:días] [/uniquepw:número] [/domain]

net accounts [/sync] [/domain]

Párametro	Significado
Ninguno	Presenta en pantalla las configuraciones actuales de contraseña, limitaciones de inicio de sesión e información de dominio.
/forcelogoff:{minutos | no}	Establece el número de minutos que transcurrirán antes de que se dé por finalizada una sesión de usuario en un servidor tras el vencimiento de la cuenta de usuario o el tiempo válido de inicio de sesión. Con la opción no se impide que se produzca un cierre de sesión forzado. El valor predeterminado es 'no'. Cuando se especifica la opción /forcelogoff:minutos, WinNT envía una advertencia minutos antes de forzar la salida del usuario de la red. Si hay algún archivo abierto, WinNT advierte al usuario. Si minutos es menor que dos,WinNT indica al usuario que cierre la sesión de red inmediatamente.
/minpwlen:longitud	Establece el número mínimo de caracteres para la contraseña de una cuenta de usuario. Los valores válidos oscilan entre 0 y 14 caracteres; el valor predeterminado es de 6 caracteres.

/maxpwage:{días | unlimited}	Establece el número máximo de días de validez de la contraseña de una cuenta de usuario. El valor 'unlimited' establece un tiempo ilimitado. La opción /maxpwage debe ser mayor que /minpwage. Los valores válidos oscilan entre 1 y 49710 días (unlimited); el valor predeterminado es de 90 días.
/minpwage: días	Establece el número mínimo de días que han de transcurrir antes de que un usuario pueda cambiar una contraseña nueva. Un valor 0 significa que no hay tiempo mínimo. Los valores válidos oscilan entre 0 y 49710 días; el valor predet. es de 0 días.
/uniquepw:número	Impide que el usuario repita la misma contraseña durante número cambios de contraseña. Los valores válidos oscilan entre 0 y 8 cambios de contraseña; el valor predeterminado es de 5 cambios.
/domain	Realiza la operación sobre el controlador principal del dominio actual. Si no se especifica este parámetro, la operación se realizará en el equipo local. (Este parámetro se aplica únicamente a equipos con Windows NT Workstation que son miembros de un dominio de WinNT Server. De manera predeterminada, los equipos con WinNT Server realizan las operaciones sobre el controlador principal del dominio).
/sync	Cuando se utiliza en el controlador principal de dominio, causa la sincronización de todos los controladores de reserva de dicho dominio. Cuando se utiliza en un controlador de reserva, causa la sincronización de ese controlador de reserva con el controlador principal de dominio únicamente. Este comando sólo se aplica a los equipos que son miembros de un dominio de WinNT Server.

Ejemplos:

- Para mostrar la configuración actual para el cierre forzado de sesión, los requisitos de contraseña y la función de un servidor determinado.	net accounts
- Para establecer un mínimo de siete caracteres para las contraseñas de la cuenta de usuario.	net accounts /minpwlen:7
- Para especificar que una contraseña no pueda repetirse hasta pasados cinco cambios	net accounts /uniquepw:5
- Para evitar que los usuarios cambien la contraseña con una frecuencia mayor que cada 7 días, para forzar el cambio de contraseña cada 30 días y para forzar el cierre de sesión tras el vencimiento del tiempo de inicio de sesión y emitir una advertencia 5 minutos antes del cierre forzado	net accounts /minpwage:7 /maxpwage:30 /forcelogoff:5

- Para realizar la tarea anterior en un equipo con Windows NT Workstation y asegurarse de que la configuración es efectiva en el dominio de Windows NT Server en el que el equipo ha iniciado la sesión.	net accounts /minpwage:7 /maxpwage:30 /domain
Para actualizar la base de datos de cuentas de usuario de todos los servidores miembros.	net accounts /sync

'Net Computer'

Agrega o elimina equipos de una base de datos de dominios. Este comando está disponible sólo en los equipos con Windows NT Server.

net computer \\equipo {/add | /del}

Parametro	Significado
\\equipo	Especifica el equipo que se agrega o elimina del dominio.
/add	Agrega el equipo especificado al dominio.
/del	Quita el equipo especificado del dominio.

Ejemplo:

- Para agregar el equipo ARCOIRIS al dominio.	net computer \\arcoiris /add

'Net Config'

Muestra los servicios configurables que están en ejecución, o muestra y modifica la configuración de un servicio.

net config [servicio [opciones]]

Parametro	Significado
ninguno	Escriba net config sin parámetros para ver una lista de los servicios configurables.
Servicio	Es un servicio (server o workstation) que puede configurarse con el comando net config.
Opciones	Son específicas del servicio. Vea net config server o net config workstation para obtener la sintaxis completa

Use el comando net config servicio para cambiar parámetros configurables de servicio Servidor o Estación de trabajo. Los cambios entran en vigor inmediatamente y son permanentes.

'Net Config Server'

Muestra o cambia la configuración para el servicio Servidor mientras dicho servicio está en ejecución.

net config server [/autodisconnect:tiempo] [/srvcomment:"texto "] [/hidden:{yes | no}]

Parametro	Significado
ninguno	Visualiza la configuración actual del servicio Servidor.
/autodisconnect :tiempo	Establece el número máximo de minutos que una sesión de usuario puede permanecer inactiva antes de que se desconecte. Puede especificar -1 para que nunca se produzca dicha desconexión. Los valores válidos oscilan entre -1 y 65535 minutos;el valor predeterminado es 15.

/srvcomment: "texto"	Agrega un comentario para el servidor que se muestra en las pantallas de WinNT y con el comando net view. El comentario puede tener un máximo de 48 caracteres. Escriba el texto entre comillas.
/hidden:{yes | no}	Especifica si el nombre de equipo del servidor debe aparecer al presentar la lista de servidores. Tenga en cuenta que el hecho de ocultar un servidor no modifica los permisos definidos en él. El valor predeterminado es 'no'.

Ejemplos:

- Para mostrar información acerca del servidor local e impedir que la pantalla se desplace.	net config server | more
- Para ocultar el nombre de equipo del servidor en la lista de servidores disponibles.	net config server /hidden:yes
- Para desconectar a un usuario después de 15 minutos de inactividad.	net config server /autodisconnect:15

'Net Config Workstation'

Muestra o cambia la configuración del servicio Estación de trabajo mientras está en ejecución.

net config workstation [/charcount:bytes] [/chartime:ms] [/charwait:s]

Parámetro:	Significado:
Ninguno	Escriba net config workstation para mostrar la configuración actual del equipo local.

Parametro	Significado
/charcount:bytes	Especifica la cantidad de datos que recopila WinNT antes de enviarlos a un dispositivo de comunicaciones. Si se establece también /chartime:ms, WinNT actúa según la condición que se satisfaga primero. Los valores válidos oscilan entre 0 y 65.535 bytes; el valor predeterminado es de 16 bytes.
/chartime:ms	Establece el número de milisegundos durante los cuales WinNT recopila datos antes de enviarlos a un dispositivo de comunicaciones. Si se establece también /charcount:bytes, WinNT actúa según la condición que se satisfaga primero. Los valores válidos oscilan entre 0 y 65.535.000 milisegundos; el valor predeterminado es de 250 milisegundos.
/charwait:seg	Establece el número de segundos que esperará WinNT a que un dispositivo de comunicaciones esté disponible. Los valores válidos oscilan entre 0 y 65.535 segundos; el valor predeterminado es de 3.600 segundos.

Ejemplos:

- Para presentar en pantalla la configuración actual del servicio Estación de trabajo	net config workstation

- Para establecer el número de milisegundos que WinNT espera antes de enviar los datos a un dispositivo de comunicación a 500 milisegundos	net config workstation /chartime:500

'Net Continue'

Vuelve a activar un servicio interrumpido.

net continue servicio

Parametro	Significado
Servicio	Los servicios que pueden reanudarse son los siguientes: servidor de archivos para macintosh (sólo para WinNT Server),servicio de publicación de FTP, lpdsvc, inicio de sesión de red, dde de red, dsdm dde de red, proveedor de seguridad nt lm, inicio remoto(sólo para WinNT Server), servidor de acceso remoto, schedule, servidor, servicios simples de tcp/ip y estación de trabajo.

'Net File'

Muestra los nombres de todos los archivos compartidos abiertos en un servidor y el número de bloqueos de archivo (si existe alguno) en cada uno de ellos. Este comando también cierra archivos compartidos individuales y quita bloqueos de archivo.

net file [id [/close]]

Parametro	Significado
ninguno	Escriba net file sin parámetros para obtener una lista de los archivos abiertos en un servidor.
Id	Es el número de identificación del archivo.
/close	Cierra un archivo abierto y libera los registros bloqueados. scriba este comando desde el servidor en el que se comparte el archivo.

Ejemplos:

- Para ver una pantalla de información acerca de los archivos compartidos	net file
- Para cerrar un archivo con el número de identificación 1	net file 1 /close

La pantalla que muestra el comando net file es similar a la siguiente:

Archivo	Ruta de acceso	Nombre de usuario	Bloqueos
0	C:\ARCH_A.TXT	MARISAF	0
1	C:\BASEDATOS	DAVIDSA	2

'Net Group'

Agrega, muestra o modifica grupos globales en dominios de Windows NT Server. Este comando sólo está disponible en los dominios de Windows NT Server.

net group [nombre_grupo [/comment:"texto"]] [/domain]

net group nombre_grupo {/add [/comment:"texto"] | /delete} [/domain]

net group nombre_grupo nombre_usuario[...] {/add | /delete} [/domain]

Parametro	Significado
ninguno	Escriba net group sin parámetros para mostrar e nombre de un servidor y los nombres de los grupos de dicho servidor.
nombre_grupo	Es el nombre del grupo que va a agregarse, expandirse o eliminarse. Especifique un nombre de grupo para ver la lista de los usuarios correspondientes.
/comment: "texto"	Agrega un comentario para un grupo nuevo o existente. Dicho comentario puede tener hasta 48 caracteres. Escriba el texto entre comillas.
/domain	Realiza la operación sobre el controlador principal del dominio actual. Si no se especifica este parámetro, la operación se realizará en el equipo local. Este parámetro se aplica únicamente a equipos con WinNT Workstation que son miembros de un dominio de WinNT Server. De manera predeterminada, los equipos con WinNT Server realizan las operaciones en el controlador principal del dominio.
nombre_usuario [...]	Muestra la lista de uno o más usuarios que se agregarán o quitarán de un grupo. Separe los nombres de usuario con un espacio en blanco.

Parametro	Significado
/add	Agrega un grupo o un nombre de usuario a un grupo. Debe establecerse una cuenta para los usuarios agregados a un grupo con este comando.
/delete	Quita un grupo o un nombre de usuario de un grupo.

Ejemplos:	
- Para ver una lista de todos los grupos en el servidor local	net group
- Para agregar un grupo llamado ejec a la base de datos local de cuentas de usuario	net group ejec /add
- Para agregar un grupo llamado ejec a la base de datos de cuentas de usuario de un dominio de Windows NT Server desde un equipo con el software Windows NT Workstation instalado	net group ejec /add /domain
Para agregar las cuentas de usuario ya existentes esterv, rafar y jesust al grupo ejec en el equipo local	net group ejec esterv rafar jesust /add
- Para agregar las cuentas de usuario ya existentes esterv, rafar y jesust al grupo ejec de un dominio de Windows NT Server desde un equipo con el software Windows NT Workstation instalado	net group ejec esterv rafar jesust /add /domain
- Para mostrar los usuarios del grupo ejec	net group ejec
- Para agregar un comentario al registro del grupo ejec	net group ejec /comment:"Plantilla de jecutivos"

La pantalla que muestra los grupos del servidor es similar a la siguiente:

Cuentas de grupo de \\PRODUCCIÓN

*Admins. del dominio *Usuarios del dominio

Observe que los nombres de grupos van precedidos por un asterisco (*), que sirve para identificar los grupos que incluyen usuarios y grupos.

'Net Help'

Proporciona una lista de comandos de red y temas sobre los que puede obtener ayuda, o proporciona ayuda acerca de un comando o tema específico. Los comandos de red disponibles también se muestran en la ventana Comandos de esta Referencia de comandos, bajo la letra N.

net help [comando]
net comando {/help | /?}

Parametro	Significado
ninguno	Escriba net help sin parámetros para mostrar una lista de comandos y temas acerca de los cuales puede obtenerse ayuda.
comando	Es el comando acerca del cual desea obtener ayuda. No escriba net como parte del comando.
/help	Proporciona una forma alternativa de mostrar en pantalla el texto de ayuda.
/?	Muestra la sintaxis correcta del comando.

Ejemplos:

- Para obtener la misma información acerca del comando net use, utilizando dos formas del comando net help	net help use o bien net use /help
- Para ver la sintaxis del comando net use	net use /?

'Net Helpmsg'

Proporciona ayuda referente a un mensaje de error de Windows NT.

net helpmsg mensaje_nº

Parametro	Significado
mensaje_nº	Es el número de cuatro dígitos del mensaje de WinNT acerca del cual necesita ayuda.

'Net Localgroup'

Agrega, muestra o modifica grupos locales.

net localgroup [nombre_grupo [/comment:"texto"]] [/domain]

net localgroup nombre_grupo {/add [/comment:"texto"] | /delete} [/domain]

net localgroup nombre_grupo nombre [...] {/add | /delete} [/domain]

Parametro	Significado
Ninguno	Escriba net localgroup sin parámetros para mostrar el nombre del servidor y los nombres de los grupos locales de dicho equipo.
Nombre_grupo	Es el nombre del grupo que va a agregarse, expandirse o eliminarse. Proporcione sólo un nombre_grupo para

Parametro	Significado
	ver una lista de los usuarios o grupos globales de un grupo local.
/comment: "texto"	Agrega un comentario para un grupo nuevo o existente. El comentario puede tener hasta 48 caracteres de longitud. Escriba el texto deseado entre comillas.
/domain	Realiza la operación en el controlador principal del dominio actual. Si no se especifica este parámetro, la operación se realizará en el equipo local. Este parámetro se aplica únicamente a equipos con Windows NT Workstation que son miembros de un dominio de Windows NT Server. Si no se indica lo contrario, los equipos con WinNT Server realizarán las operaciones en el controlador principal del dominio.
Nombre [...]	Muestra la lista de uno o más nombres de usuario o de grupo que se agregarán a un grupo local o se quitarán de él. Separe cada nombre con un espacio en blanco. Los nombres pueden ser usuarios locales, usuarios de otros dominios o grupos globales, pero no otros grupos locales. Si un usuario es de otro dominio, escriba el nombre de usuario después del nombre de dominio (por ejemplo, VENTAS\SAMUEL).
/add	Agrega un nombre de grupo o de usuario a un grupo local. Debe establecerse una cuenta para los usuarios o grupos globales que se agreguen a un grupo local con este comando.
/delete	Quita un nombre de grupo o de usuario de un grupo local.

Use el comando net localgroup para agrupar usuarios que utilizan de un modo igual o similar el equipo o la red. Cuando se asignen derechos a un grupo local, cada miembro de dicho grupo recibirá automáticamente estos derechos.

Ejemplos:	
- Para mostrar una lista de todos los grupos locales del servidor local	net localgroup
- Para agregar un grupo local llamado ejec a la base de datos local de cuentas de usuario	net localgroup ejec /add
- Para agregar un grupo local llamado ejec a la base de datos de cuentas de usuario de un dominio de WinNT Server	net localgroup ejec /add /domain
- Para agregar las cuentas de usuario ya existentes esterv, rafar (del dominio VENTAS) y jesust al grupo local ejec en el equipo local	net localgroup ejec esterv ventas\rafar jesust /add
- Para agregar las cuentas de usuario ya existentes esterv, rafar y jesust al grupo ejec de un dominio de WinNT Server	net localgroup ejec esterv rafar jesust /add /domain

Ejemplos:	
- Para agregar un comentario al registro del grupo local ejec	net localgroup ejec /comment:"Plantilla de ejecutivos"

'Net Name'

Agrega o elimina un nombre para mensajes (a veces llamado alias), o muestra la lista de nombres para los que el equipo aceptará mensajes. Para poder usar net name, el servicio de Mensajería debe estar en ejecución.

net name [nombre [/add | /delete]]

Parametro	Significado
ninguno	Escriba net name sin parámetros para mostrar una lista de los nombres actualmente en uso.
nombre	Especifica el nombre que recibe mensajes. Dicho nombre puede tener un máximo de 15 caracteres.
/add	Agrega un nombre a un equipo. Escribir /add es opcional puesto que el resultado de escribir net name nombre es el mismo que el de escribir net name nombre /add.
/delete	Quita un nombre de un equipo.

Ejemplos:	
- Para ver la lista de nombres en su equipo	net name
- Para agregar el nombre rsvp a su equipo	net name rsvp

Ejemplos:	
- Para quitar el nombre rsvp de su equipo	net name rsvp /delete

'Net Pause'

Interrumpe los servicios en ejecución.

net pause servicio

Parametro	Significado
servicio	Puede ser: -Servidor de archivos para Macintosh -Servicio de publicación de FTP -LPDSVC -Inicio de sesión de red -DDE de red -DSDM DDE de red -Proveedor de seguridad Lan Manager de NT -Inicio remoto (sólo en Windows NT Server) -Servidor de acceso remoto -Schedule -Servidor -Servicios simples de tcp/ip -Estación de trabajo.

Ejemplos:	
- Para interrumpir el servicio Servidor	net pause server
- Para interrumpir el servicio Inicio de sesión de red	net pause "net logon"

'Net Print'

Muestra o controla los trabajos y las colas de impresión.

net print \\nombre_equipo\recurso_compartido

net print [\\nombre_equipo] trabajo_nº [/hold | /release | /delete]

Parametro	Significado
Nombre_equipo	Es el nombre del equipo que comparte las colas de impresión.
Recurso_compartido	Es el nombre de la cola de impresión.
Trabajo_nº	Cuando incluya recurso_compartido y nombre_equipo, sepárelos con una barra invertida (\).
/hold	Es el número de identificación asignado a un trabajo de impresión en una cola. Cuando se usa con trabajo_nº, retiene el trabajo en espera en la cola de impresión. El trabajo permanece en la cola y los demás trabajos lo rebasarán hasta que se libere.
/release	Libera un trabajo o una cola de impresión que se ha retenida.
/delete	Quita un trabajo de la cola de impresión.

Ejemplos:

- Para obtener información acerca del trabajo número 35 del equipo \\PRODUCCIÓN	net print \\producción 35
- Para retener el trabajo número 263 del equipo \\PRODUCCIÓN	net print \\produccion 263 /hold
- Para liberar el trabajo número 263 del equipo \\PRODUCCIÓN	net print \\producción 263 /release
- Para obtener una lista del contenido de la cola de impresión MATRIZ del equipo \\PRODUCCIÓN	net print \\producción\ matriz

Lo siguiente es un ejemplo de la información presentada de todas las colas de impresión:

Colas de impresora en \\PRODUCCIÓN

Nombre	Trabajo No.	Tamaño	Estado
Cola LÁSER	1 trabajos		*Cola activa*
	1 trabajos	0	en cola

Use net print trabajo_nº para mostrar un único trabajo de impresión. Aparecerá una pantalla similar a la siguiente:

Trabajo No.	35
Estado	Esperando
Tamaño	3096
Comentario	
Usuario	MARIASL
Notificar	MARIASL
Tipo de dato del trabajo	
Parámetros del trabajo	
Información adicional	

'Net Send'

Envía mensajes a otros usuarios, equipos, grupos o nombres para mensajes en la red. El servicio Mensajería debe estar en ejecución para poder recibir mensajes.

net send {nombre | * | /domain[:nombre] | /users} mensaje

Parametro	Significado
nombre	Es el nombre de usuario, de equipo o nombre para mensajes al que se envía el mensaje. Si se trata de un nombre de equipo que contiene caracteres en blanco, escríbalo entre comillas (" ").
*	Envía el mensaje a todos los nombres del grupo.

Parametro	Significado
/domain [:nombre]	Envía el mensaje a todos los nombres del dominio del equipo. Si se especifica nombre, se enviará el mensaje a todos los nombres del dominio o grupo de trabajo especificado.
/users	Envía el mensaje a todos los usuarios conectados al servidor.
mensaje	Es el texto que se enviará como mensaje.

Ejemplos:

- Para enviar el mensaje "Reunión cambiada a las 15 horas. En el mismo lugar." al usuario robertof, escriba:	net send robertof Reunión cambiada a las 15 horas. En el mismo lugar.
- Para enviar un mensaje a todos los usuarios conectados al servidor, escriba:	net send /users Este servidor se apagará en 5 minutos.
- Para enviar un mensaje que incluya una barra diagonal, escriba:	net send robertof "Formatear tu disco con FORMAT /4"

'Net Session'

Muestra la lista o desconecta las sesiones entre un equipo local y los clientes conectados a él.

net session [\\nombre_equipo] [/delete]

Parametro	Significado
Ninguno	Escriba net session sin parámetros para que se muestre información acerca de todas las sesiones con el equipo local.
\\nombre_equipo	Identifica el equipo para el cual se mostrarán o desconectarán sesiones.
/delete	Finaliza la sesión del equipo con \\nombre_equipo y cierra todos los archivos abiertos en el equipo para la sesión. Si se omite \\nombre_equipo, se cancelarán todas las sesiones del equipo local.

Ejemplos:

- Para mostrar una lista con información sobre las sesiones del servidor local	net session
- Para mostrar información sobre las sesiones del cliente cuyo nombre de equipo es SÁNCHEZ	net session \\sánchez
- Para finalizar todas las sesiones entre el servidor y los clientes conectados	net session /delete

La pantalla es similar a la siguiente:

Equipo	Usuario	Tipo de cliente	Abiertos	Inactiva
\\BASSETT	CRISDR	NT	1	00:00:13
\\SANZCA	Administrador	DOS LM 2.1	0	01:05:13

'Net Share'

Crea, elimina o muestra recursos compartidos.
net share recurso_compartido
net share recurso_compartido =unidad:ruta_de_acceso [/users:número | /unlimited] [/remark:"texto"]
net share recurso_compartido [/users:número

| unlimited] [/remark:"texto"]

net share {recurso_compartido | unidad :ruta_de_acceso} /delete

Párametro	Significado
Ninguno	Escriba net share sin parámetros para mostrar información acerca de todos los recursos compartidos en el equipo local.
recurso_compartido	Es el nombre de red del recurso compartido. Escriba 'net share' con un recurso_compartido únicamente para mostrar información acerca de dicho recurso compartido.
unidad:ruta_de_acceso	Especifica la ruta de acceso absoluta del directorio que va a compartirse.
/users:número	Establece el número máximo de usuarios que pueden tener acceso simultáneamente al recurso compartido.
/unlimited	Especifica que puede tener acceso simultáneamente al recurso compartido un número ilimitado de usuarios.
/remark:"texto"	Agrega un comentario descriptivo acerca del recurso. Escriba el texto entre comillas.
/delete	Deja de compartir un recurso.

Ejemplos:

- Para mostrar información acerca de los recursos compartidos en el equipo	net share
- Para compartir el directorio C:\CARTAS de un equipo con el nombre compartido SECRETARIA e incluir un comentario	net share secretaria=c:\cartas /remark: "Para el departamento 123"
- Para dejar de compartir el directorio CARTAS	net share secretaria /delete
- Para compartir el directorio C:\LST FIG de un equipo con el nombre compartido LISTA	net share lista= "c:\lst fig"

La presentación en pantalla es similar a la siguiente:

Nombre	Recurso	Comentario
ADMIN$	C:\WINNT	Admin Remota
C$	C:\	Uso interno
print$	C:\WINNT\SYSTEM\SPOOL	
IPC$	IPC remota	
LÁSER	LPT1 En cola	Impresora Láser

'Net Start'

Inicia un servicio o muestra una lista de los servicios iniciados. Los nombres de servicios que son de dos o más palabras, como Inicio de sesión de red o Examinador de equipos, deben estar entre comillas (").

net start [servicio]

Parametro	Significado
ninguno	Escriba net start sin parámetros para mostrar una lista de los servicios en ejecución.

servicio Puede ser: Alerta
Servicio de cliente para netware
Servidor del Portafolio
Examinador de equipos
Cliente dhcp
Duplicador de directorios
Registro de sucesos
Servicio de publicación de FTP
LPDSVC
Mensajería
Inicio de sesión de red
DDE de red
DSDM DDE de red
Agente de supervisión de red
Proveedor de seguridad nt lm
OLE
Administrador de conexiones de acceso remoto
Servicio isnsap de acceso remoto
Servidor de acceso remoto
Localizador de llamada a procedimientos remotos (rpc)
Servicio de llamada a procedimientos remotos (rpc)
Schedule
Servidor
Servicios simples de tcp/ip
SNMP
Spooler
Ayuda de netbios de tcp/ip
SAI
Estación de trabajo

Los siguientes servicios sólo están disponibles en Windows NT Server:
Servidor de archivos para Macintosh
Servicio de puerta de enlace o gateway para netware
Servidor de DHCP de Microsoft
Servidor de impresión para Macintosh
Inicio remoto
Servicio de nombres Internet de Windows

'Net Statistics'

Muestra el registro de estadísticas del servicio local Estación de trabajo o Servidor.

net statistics [workstation | server]

Parametro	Significado
ninguno	Escriba net statistics sin parámetros para obtener una lista de los servicios en ejecución para los cuales hay datos estadísticos disponibles.
workstation	Muestra los datos estadísticos del servicio local Estación de trabajo.
Server	Muestra los datos estadísticos del servicio local Servidor.

Ejemplos:

- Para mostrar los servicios en ejecución para los que hay estadísticas disponibles	net stats
- Para mostrar las estadísticas del servicio Servidor y evitar que se desplace la pantalla	net statistics server | more

'Net Stop'

Detiene un servicio de Windows NT.

net stop servicio

Servicio puede ser(ver NET START)

'Net Time'

Sincroniza el reloj del equipo con el de otro equipo o dominio. Si se utilizasin la opción /set, muestra la hora de otro equipo o dominio.
net time [\\nombre_equipo | /domain[:nombre]] [/set]

Parametro	Significado
\\nombre_equipo	Es el nombre del servidor que desee comprobar o con el que desee sincronizar las estaciones de trabajo.
/domain [:nombre]	Es el dominio con el que desea sincronizar la hora.
/set	Sincroniza el reloj del equipo con el del equipo o dominio especificado.

'Net Use'

Conecta o desconecta un equipo de un recurso compartido o muestra información acerca de las conexiones del equipo. También controla las conexiones de red persistentes.

net use [nombre_dispositivo] [\\nombre_equipo\recurso_compartido[\volumen]][contraseña | *]] [/user:[nombre_dominio\]nombre_usuario] [[/delete] | [/persistent:{yes | no}]]

net use nombre_dispositivo [/home[contraseña | *]] [/delete:{yes | no}]

net use [/persistent:{yes | no}]

Parametro	Significado
ninguno	Escriba net use sin parámetros para obtener una lista de las conexiones de red.
nombre_dispositivo	Asigna un nombre para la conexión al recurso o especifica el dispositivo que se va a desconectar. Hay dos tipos de nombres de dispositivos: unidades de disco(D a Z) e impresoras (LPT1 a LPT3). Escriba un asterisco en lugar de un nombre específico de dispositivo para asignar el siguiente nombre de dispositivo disponible.
\\nombre_equipo\recurso_compartido	Es el nombre del servidor y del recurso compartido. Si el nombre de equipo contiene caracteres en blanco, escriba la barra invertida doble (\\) y el nombre entre comillas (" "). El nombre de equipo puede tener entre 1 y 15 caracteres.
\volumen	Especifica un volumen NetWare del servidor. Para poder conectarse con servidores NetWare debe tener instalado y estar ejecutando el Servicio de cliente para NetWare (Windows NT Workstation) o el Servicio de puerta de enlace o gateway para NetWare (WinNT Server).
contraseña	Es la contraseña necesaria para tener acceso a recurso compartido.
*	Pide por la contraseña. Los caracteres no se muestran en pantalla a medida que los escribe.
/user	Especifica un nombre de usuario diferente con el que se realiza la conexión.
nombre_dominio	Especifica otro dominio. Por ejemplo, net use d: \\servidor\recurso_compartido /user:admin\mario conecta el usuario mario de

	la misma forma que si la conexión se realizara desde el dominio administrador. Si se omite el dominio, se usará aquél en el que tenga lugar la conexión actual.	Ejemplos: - Para asignar el nombre de dispositivo de unidad de disco E: al directorio compartido CARTAS del servidor \\FINANCIERO	net use e: \\financiero\cartas
nombre_usuario	Especifica el nombre de usuario con el que se iniciará la sesión.	- Para asignar el nombre de dispositivo de unidad de disco M: al directorio MARÍA dentro del volumen CARTAS del servidor NetWare FINANCIERO	net use m: \\financiero\cartas\maría
/home	Conecta un usuario con su directorio particular.		
/delete	Cancela la conexión de red especificada. Si el usuario especifica la conexión mediante un asterisco se cancelarán todas las conexiones de red.	- Para asignar el nombre de dispositivo LPT1 a la cola de la impresora compartida LÁSER2 del servidor \\CONTABILIDAD	net use lpt1: \\contabilidad\láser2
		- Para desconectarse de la cola de impresora LPT1	net use lpt1: /delete
/persistent	Controla el uso de conexiones de red persistentes. El valor predeterminado es la última configuración utilizada. Las conexiones sin dispositivos no son persistentes.	- Para asignar el nombre de dispositivo de unidad de disco H: al directorio particular del usuario mario /user:mario	net use h: \\contabilidad\usuarios /home /user:mario
Yes	Guarda todas las conexiones tal como se realizaron y las restaura en el siguiente inicio de sesión.	- Para asignar el nombre de dispositivo de unidad de disco F: al directorio compartido NOTAS del servidor \\FINANCIERO, que requiere la contraseña hctarcs, sin que la conexión sea persistente	net use f: \\financiero\notas hctarcs /persistent:no
No	No guarda la conexión en curso ni las siguientes. Las existentes se restaurarán en el siguiente inicio de sesión. Use el modificador /delete para eliminar conexiones persistentes.	- Para desconectarse del directorio \\FINANCIERO\NOTAS	net use f: \\financiero\notas /delete
		- Para conectarse a un recurso compartido del servidor FINANCIERO2	net use k: "\\financiero2"\circulares

-Para restaurar las conexiones actuales cada vez que se inicie una sesión, independientemente de cambios futuros	net use /persistent:yes

'Net User'

Agrega o modifica cuentas de usuario o muestra información acerca de ellas.

net user [nombre_usuario [contraseña | *] [opciones]] [/domain]

net user nombre_usuario {contraseña | *} /add [opciones] [/domain]

net user nombre_usuario [/delete] [/domain]

Párametro	Significado
Ninguno	Escriba net user sin parámetros para ver una lista de las cuentas de usuario del equipo.
Nombre_usuario	Es el nombre de la cuenta de usuario que se desea agregar, eliminar, modificar o ver. El nombre de la cuenta de usuario puede tener hasta 20 caracteres.
contraseña	Asigna o cambia una contraseña para la cuenta de usuario. Una contraseña debe tener la longitud mínima establecida con la opción /minpwlen del comando net accounts y puede tener un máximo de 14 caracteres.
*	Pide la contraseña. Los caracteres no se muestran en pantalla a medida que los escribe.
/domain	Realiza la operación en el controlador principal del dominio principal del equipo. Este parámetro se aplica únicamente a equipos con WinNTWorkstation que son miembros de un dominio de Windows NT Server. De forma predeterminada, los equipos con Windows NT Server realizan las operaciones en el controlador principal de dominio.
/add	Agrega una cuenta de usuario a la base de datos de cuentas de usuario.
/delete	Quita una cuenta de usuario de la base de datos de cuentas de usuario.

Opciones	Significado
/active:{no | yes}	Desactiva o activa la cuenta de usuario. Si no está activa, el usuario no puede tener acceso a los recursos del equipo. El valor predeterminado es 'yes' (activa).
/comment: "texto"	Proporciona un comentario descriptivo acerca de la cuenta de usuario.Puede tener hasta 48 caracteres. Escriba el texto entre comillas.
/countrycode: nnn	Usa los códigos de país del sistema operativo para instalar los archivos de ayuda y mensajes de error en el idioma especificado. Un valor 0 significa el código de país predeterminado.

/expires:{fecha | never}	El parámetro fecha establece una fecha de caducidad de la cuenta de usuario, mientras que never determina una duración ilimitada de dicha cuenta. Las fechas de caducidad pueden darse en el formato mm/dd/aa, dd/mm/aa o mm,dd,aa, dependiendo de /countrycode. Observe que la cuenta caduca al comienzo de la fecha especificada. Los meses pueden indicarse con un número, con todas sus letras o abreviados con tres letras. Los años pueden constar de dos o cuatro dígitos. Utilice comas o barras diagonales para separar las partes de la fecha (no espacios en blanco). Si se omite aa, se asume el año de la siguiente fecha (de acuerdo con la fecha y hora de su equipo).
/fullname:"nombre"	Agrega un determinado nombre al usuario en lugar de su nombre de usuario normal. Escriba dicho nombre entre comillas.
/homedir:ruta_acceso	Establece la ruta de acceso del directorio particular del usuario. Dicha ruta debe ser una ya existente.
/homedirreq:{yes | no}	Establece si es necesario un directorio particular.
/passwordchg:{yes | no}	Especifica si los usuarios pueden cambiar su contraseña. El valor predeterminado es 'yes'.
/passwordreq:{yes | no}	Especifica si una cuenta de usuario debe tener una contraseña. El valor predeterminado es 'yes'.
/profilepath[:ruta_acceso]	Establece una ruta de acceso para el perfil de inicio de sesión del usuario. Dicha ruta lleva a un perfil de registro.
/scriptpath:ruta_acceso	Establece una ruta de acceso al archivo de comandos de inicio de sesión del usuario. Ruta_acceso no puede ser una ruta absoluta; es relativa a%raíz_sistema%\SYSTEM32\REPL\IMPORT\SCRIPTS.
/times:{horas | all}	Especifica las horas en las que se permite al usuario el uso del equipo. El valor horas se expresa como día[-día][,día[-día]],hora[-hora][,hora[-hora]], limitado a incrementos de una hora. Los días se pueden deletrear o abreviar (L,M,Mi,J,V,S,D). Las horas se pueden escribir en formato de 12 ó 24 horas. Para el formato de 12 horas, use AM, PM, o A.M., P.M. El valor 'all' significa que un usuario puede iniciar una sesión en cualquier momento. Un valor nulo (en blanco)significa que un usuario nunca puede iniciar la sesión. Separe el día y la hora mediante comas, y las unidades de día y hora con punto y coma (por ejemplo, L,4AM-5PM;M,1AM-3PM). No use espacios en la especificación de /times.

/usercomment:"texto"	Permite que un administrador agregue o cambie el "Comentario de usuario"de la cuenta. Escriba el texto entre comillas.

'Net View'

Muestra una lista de dominios, una lista de equipos o los recursos compartidos en el equipo especificado.

net view [\\nombre_equipo | /domain[:nombre_dominio]]

net view /network:nw [\\nombre_equipo]

Parametro	Significado
ninguno	Escriba net view sin parámetros para mostrar la lista de los equipos del dominio actual.
nombre_equipo	Especifica el equipo cuyos recursos compartidos desea ver.
/domain[:nombre_dominio]	Especifica el dominio del que se desean ver los equipos disponibles. Si se omite nombre_dominio, se mostrarán todos los dominios de la red.
/network:nw	Muestra todos los servidores disponibles de una red NetWare. Si se especifica un nombre de equipo, se mostrarán los recursos disponibles en dicho equipo de la red NetWare. Mediante esta opción también pueden especificarse otras redes que se hayan agregado al sistema.

Ejemplos:	
- Para ver una lista de los recursos compartidos por el equipo \\PRODUCTOS, escriba:	net view \\productos
- Para ver los recursos disponibles en el servidor NetWare \\MARKETING, escriba	net view /network:nw \\marketing
- Para ver una lista de los equipos del dominio o grupo de trabajo Ventas, escriba:	net view /domain:ventas

Use el comando net view para mostrar una lista de equipos similar a
la siguiente:

Nombre de servidor	Comentario
\\PRODUCCIÓN	Servidor de archivos de Producción
\\PRINT1	Sala de impresoras, primer piso
\\PRINT2	Sala de impresoras, segundo piso

HACK-OPINION
PAGOS POR INTERNET SEGUROS YA

AZIMUT y yo hace tiempo que mantenemos acaloradas "discusiones" sobre muchos temas relacionados con las "nuevas tecnologías". Supongo que nos encanta debatir las cosas, pero hay algunas posiciones que compartimos y una es todo lo relacionado con el tema de los pagos por Internet.

El Problema/Los Problemas:

Actualmente, uno de los mayores impedimentos para el desarrollo del Comercio Electrónico es la sensación de inseguridad que tienen las personas cuando se ven obligadas a dar su número de tarjeta de crédito por Internet y, créeme, les entiendo perfectamente. No importa que tengas 3 antivirus y 5 firewalls en tu equipo, te aseguro que metiéndote un simple proceso en el sistema puedo tener un Log de cada tecla que pulsas en tu teclado (quedas advertido!!!).

"puedes pedirme que confíe en ti, pero no esperes que cruce la autopista de noche y con los ojos vendados"

En Internet, una vez superas el miedo a pagar por adelantado un producto que no puedes tocar y aprendes a esperar que te llegue el material por una empresa de transporte, se te pide que introduzcas el número de una tarjeta de crédito que, para colmo, está vinculada a una cuenta bancaria donde posiblemente tienes tus ahorros o cobras tu nómina. Hombre, puedes pedirme que confíe en ti, pero no esperes que cruce la autopista de noche y con los ojos vendados, ¿vale?.

En estas circunstancias es normal que el comercio electrónico no despegue, vamos, creo que a pesar de todo, desde mi punto de vista, está funcionando demasiado bien por mucho que los analistas digan que estamos no se cuantos puntos por debajo de las previsiones. Pero, ¿en qué mundo viven los analistas? ¿a quién le hacen las encuestas? A mi no, nunca me han preguntado y eso que dicen que se hacen más de 3000 encuestas al día en España de los aspectos más diversos. No se, quizás se las inventan, porque no lo entiendo.

¿Qué hacen "los grandes" para solucionar el problema?

Bueno, no podemos decir que los "gigantes" del comercio no estén haciendo nada, cada día todo es más seguro y los sistemas de pago a distancia están en continua evolución. Se están gastando verdaderas millonadas en desarrollar pasarelas de pago seguras, sistemas que garantizan la seguridad de nuestras transacciones. Eso está bien, muy bien.

Que tontos somos a veces, de verdad, pero que tontos somos!!! Lo único que hacen es inventar cómo sangrarnos a base comisiones. Que triste, están matando la gallinita de los huevos de oro antes de que ponga huevos, esto es demasiado.

- Y tú que propones, listo!!! ¿Acaso tienes una solución para disparar las compras por Internet?

La solución:

Si el problema principal es el miedo a que alguien te saquee tu cuenta corriente, pues está claro, busca un sistema para que eso sea imposible.

- Si hombre, claro, qué fácil ¿no?

Una posibilidad sería, por ejemplo, poder comprar tarjetas recargables tipo móviles, si, como las de amena, airtel, etc. El método, más sencillo imposible, tienes una tarjeta con una carga inicial de dinero (por ejemplo 30 euros) y un número identificativo, cuando quieres hacer una compra por Internet utilizas ese número identificativo y automáticamente disminuye la carga en función de tus compras. La tarjeta es completamente independiente de tu cuenta corriente, por lo que en caso de que alguien te robe la numeración, lo único que pierdes es la carga restante, nada de dar acceso a nadie a tus ahorros.

"… pero que tontos somos!!! Lo único que hacen es inventar cómo sangrarnos a base comisiones…"

Incluso, yo diría que muy tonto es el que intenta robar una tarjeta de 30 euros, no se, es bastante ridículo. Los delincuentes perderían el interés que tienen actualmente en hackear Webs para conseguir las numeraciones VISA y la gente como tú y yo perderíamos el miedo a comprar por la red.

Incluso, si me apuras, que la tarjeta se pudiese recargar en los cajeros automáticos. De esta forma podrías recargarla en cualquier cajero con 20 o 30 míseros euros y reutilizarla sin que exista una relación entre la tarjeta y la cuenta, ya sabes que este tipo de tarjetas se pueden recargar desde cualquier cuenta a la que tengas acceso.

LISTO!!!, ya hemos impulsado el Comercio Electrónico.

¿Por qué no implantan este método?

Pues no lo se, sinceramente, yo incluso diría que esto no es nuevo, ni de lejos, creo recordar que antes algunas tarjetas de móviles funcionaban por este método. Así que, aquí estamos, con cientos de miles de posibles compradores esperando a que los "señores todopoderosos" implanten un sistema de este tipo.



"… la solución son las tarjetas de crédito recargables…"

Está comprobado que las compras por Internet suelen ser de pequeños importes. Piensa por un momento, seguro que al igual que me ha pasado a mí te ha sucedido a ti un montón de veces. Paseas tranquilamente por una página y ves algo que realmente te interesa, por ejemplo una suscripción, pero cuando vas a suscribirte te encuentras que te pide la VISA o te dice que envíes un talón conformado a "ves-a-saber-donde" y que recibirás un código y tal y cual o que envíes una transferencia a no se que banco de Inglaterra, vamos, que se te quitan las ganas de inmediato.

Imagina un sistema tipo VISA (que se puede utilizar en todo el mundo) pero aplicado a tarjetas recargables, sería genial, podrías realizar una transacción económica con cualquier empresa/particular de cualquier parte del mundo, desde tu casa y sin miedo de que alguien pueda echar mano de tus ahorros. El que escribe este artículo está total y absolutamente convencido de que el Comercio Electrónico daría un salto de gigante en pocos meses.

Un saludo a los contertulios y hasta la próxima :)



LOS CUADERNOS DE
HACK X CRACK
www.hackxcrack.com

SUSCRIBETE A
PC PASO A PASO

SUSCRIPCIÓN POR:
1 AÑO
11 NUMEROS

=

45 EUROS (10% DE DESCUENTO)
+
SORTEO DE UNA CONSOLA XBOX
+
SORTEO 2 JUEGOS PC (A ELEGIR)

Contra Reembolso

Solo tienes que enviarnos un mail a preferente@hackxcrack.com indicando:
- Nombre
- Apellidos
- Dirección Completa
- Población
- Provincia
- Cógigo Postal
- Mail de Contacto y/o Teléfono Contacto
Es imprescindible que nos facilites un mail o teléfono de contacto, puesto que 24 horas después de que recibamos tu petición de subscripción te daremos un número de Cliente Preferente. Este número será utilizado para los sorteos.
- Tipo de Subscripción: CONTRAREEMBOLSO
- Número de Revista:
Este será el número a partir del cual quieres subscribirte. Si deseas (por ejemplo) subscribirte a partir del número 5 (incluido), debes poner un 5 y te enviaremos desde el 5 hasta el 15 (ambos incluidos)

APRECIACIONES:
* Junto con el primer número recibirás el abono de 45 euros, precio de la subscripción por 11 números (un año) y una carta donde se te indicará tu número de Cliente Preferente y justificante/factura de la subscripción.
* Puedes hacernos llegar estos datos POR MAIL,tal como te hemos indicado; rellenando el formulario de nuestra WEB (www.hackxcrack.com) o enviándonos una carta a la siguiente dirección:
CALLE HIGINIO ANGLES Nº2, 4º-1ª
CP 43001 TARRAGONA
ESPAÑA
* Cualquier consulta referente a las subscripciones puedes enviarla por mail a preferente@hackxcrack.com

Giro Postal

Envíanos un GIRO POSTAL por valor de 45 EUROS a:
CALLE HIGINIO ANGLES Nº2, 4º-1ª
CP 43001 TARRAGONA
ESPAÑA
IMPORTANTE: En el TEXTO DEL GIRO escribe un mail de contacto o un número de Teléfono.

Y enviarnos un mail a preferente@hackxcrack.com indicando:
- Nombre
- Apellidos
- Dirección Completa
- Población
- Provincia
- Cógigo Postal
- Mail de Contacto y/o Teléfono Contacto
Es imprescindible que nos facilites un mail o teléfono de contacto, puesto que 24 horas después de que recibamos tu petición de subscripción te daremos un número de Cliente Preferente. Este número será utilizado para los sorteos.
- Tipo de Subscripción: GIRO POSTAL
- Número de Revista:
Este será el número a partir del cual quieres subscribirte. Si deseas (por ejemplo) subscribirte a partir del número 5 (incluido), debes poner un 5 y te enviaremos desde el 5 hasta el 15 (ambos incluidos)

APRECIACIONES:
* Junto con el primer número recibirás una carta donde se te indicará tu número de Cliente Preferente y justificante/factura de la subscripción.
* Puedes hacernos llegar estos datos POR MAIL,tal como te hemos indicado; rellenando el formulario de nuestra WEB (www.hackxcrack.com) o enviándonos una carta a la siguiente dirección:
CALLE HIGINIO ANGLES Nº2, 4º-1ª
CP 43001 TARRAGONA
ESPAÑA
* Cualquier consulta referente a las subscripciones puedes enviarla por mail a preferente@hackxcrack.com